Opetusministeriö

Undervisningsministeriet

Hallinto

Varmennekorttien käyttöönotto ja ylläpito yliopistoissa

Yliopistojen yhteinen suositus. Loppuraportti

Opetusministeriön julkaisuja 2009:15

Varmennekorttien käyttöönotto ja ylläpito yliopistoissa

Yliopistojen yhteinen suositus. Loppuraportti

Opetusministeriön julkaisuja 2009:15

Urpo Kaila (toim.)

Opetusministeriö • hallinto-osasto • 2009

Undervisningsministeriet • förvaltningsavdelningen • 2009

Opetusministeriö

Undervisningsministeriet

Ministry of Education

Ministère de l'Education

Opetusministeriö / Undervisningsministeriet
Hallinto-osasto / Förvaltningsavdelningen
PL / PB 29
00023 Valtioneuvosto /Statsrådet

http://www.minedu.fi/OPM/julkaisut

Taitto / Ombrytning: Liisa Heikkilä

ISBN 978-952-485-704-8 (PDF)
ISSN 1797-9501 (verkkojulkaisu)

Opetusministeriön julkaisuja / Undervisningsministeriets publikationer 2009:15

Sisältö

1 Johdanto

1.1 Projektin tausta ja lähtökohdat

Yliopistojen tietoturvapäivillä SEC'007 17.4.2007 nousi selkeästi esiin tarve selvittää, suunnitella ja edistää yliopistojen yhtenäistä käyttöönottoa varmennekorteille. Tämän johdosta yliopistojen Sec-ryhmän työvaliokunta esitti opetusministeriölle perustettavaksi opetusministeriön koordinoimaa työryhmää, jonka tehtävänä olisi selvittää, suunnitella ja edistää virkakorttien yhtenäistä käyttöönottoa Suomen yliopistoissa.

Yhtenäistä käyttöönottoa pidettiin tärkeänä, koska kortit, niihin sidottavat varmenteet sekä palvelut, joihin korteilla (varmenteilla) tunnistaudutaan, tulisivat käyttöön kaikissa Suomen yliopistoissa mahdollisimman samansisältöisinä. Yhtenäisyys mahdollistaisi tehokkaamman hallinnan ja kehityksen, tukisi yliopistojen henkilökunnan ja opiskelijoiden liikkuvuutta yliopistojen välillä sekä parantaisi turvallisuutta.

Yliopistojen Sec-ryhmän työvaliokunta esitti, että työryhmään tulisi valita jäsenet Suomen yliopistoista niin, että jokainen korttien käyttöönottoon ja käyttöön liittyvä sidosryhmä on hyvin edustettuna (mm. henkilöstöhallinto ja lakiasiat, tietohallinto ja tietoturvallisuus).

Opetusministeriön hallinnonalan tietohallintostrategian avaintoimenpiteissä on todettu, että määritellään yhtenäiset periaatteet tunnistautumiseen, virkakorttien käyttämiseen ja niiden hallinnointiin.

ValtIT:n kärkihankkeissa on ollut työryhmän perustamisen aikana rinnakkain meneillään Virkamiehen tunnistaminen -hankkeen esiselvitys, jonka tuloksia on pyritty hyödyntämään soveltuvin osin yliopistojen varmennekorttien käyttöönotossa.

Projektin taustalla on myös ollut merkittävä aikaisemmin tehty yhteistyö liittyen korkeakoulujen Haka-luottamusverkostoon sekä henkilön sähköiseen tunnistamiseen yliopistoissa ja ammattikorkeakouluissa (HSTYA).

Projektiin on vaikuttanut merkittävästi myös valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI ja sen tuottamat ohjeet ja määräykset. Esimerkiksi Tietoturvatasot-hanke edellyttää lisääntyvässä määrin infrastruktuuria ja palveluita, jotka mahdollistavat luottamuksellisen viestinnän.

Tämän perusteella opetusministeriön ja hallinnonalan tietohallinnon johtoryhmä OpIT päätti perustaa projektin asiaa selvittämään.

1.2 Projektin tavoitteet, rajaukset ja liittymät

Työryhmää asetettaessa kukin yliopisto tahollaan pohti vaadittavien varmennekorttien käyttöönottoa ja niiden elinkaaren hallintaa. Varmennekortteja on jo käytössä yliopistoissa ja niiden käyttöä edellytetään mm. Valtiokonttorin tietyissä sovelluksissa sekä tiettyihin viranomaistoimiin liittyvän sähköpostin salauksessa. Työryhmää muodostettaessa haluttiin yhdistää voimavarat ja tehdä tarvittavat käytännön selvitykset ja ohjeet yhdessä.

Projektin tavoite oli luoda yhteinen suositus kaikille yliopistoille varmennekorttien ja valittujen varmenteiden koko elinkaaren hallinnasta.

Projektin tärkeämpiä tavoitteita oli yhteisesti määritellä palvelut, joihin virkakorttia ja varmenteita tulee soveltaa. Tuetut palvelut tuli valita perustuen riskienhallintaan (suojattavat kohteet), taloudellisiin tekijöihin ja vaatimuksenmukaisuustekijöihin kuten Valtiokonttorin linjaukset.

Tuetut palvelut tuli pyrkiä määrittelemään riittävän kattavasti palvelukuvauksen, teknisen toteutuksen, resurssien käytön sekä elinkaaren hallinnan osalta.

Projektin tavoitteena oli myös selvittää varmenteiden markkinatilannetta muutaman vuoden tähtäimelle. Lisäksi projekti selvittää eri toimittajien ja teknisten ratkaisujen tilanteen hyödyntäen tässä aiempia selvityksiä, kuten HSTYA-projektia.

Projektin toimeksiannon ulkopuolelle rajattiin mm. mobiilivarmenteet ja opiskelijoiden käyttämät kortit kuten Lyyra-kortti. Koska myös osa henkilökunnasta joissain yliopistoissa käyttää Lyyra-korttia ja käytön laajentamisesta on keskusteltu, tuli projektin kuitenkin selvittää Väestörekisterikeskuksen tuottaman laatuvarmenteen sisältävän varmennekortin ja Lyyra-kortin suhde.

Projekti pyrki määrittelemään ja priorisoimaan vähimmäispalveluita sekä mahdollisia lisäpalveluita, joita voi käyttää virkakortin avulla. Määrittely pyrittiin tekemään yhdistäen eri osapuolten tarpeita ja näkemyksiä.

Uusimpien teknisten ratkaisujen hyödyntäminen ei ollut itsetarkoitus vaan projekti pyrki löytämään kestäviä ratkaisuja, joiden avulla voidaan edetä ainakin muutama vuosi.

Lisäksi projekti seurasi korttien kilpailutustilannetta ja hankintasopimuksia.

Projektisuunnitelmassa todettiin, että projektin tulee

- Määritellä varmennekortin käytön keskeiset palvelut, hyödyt ja kustannukset
- Luoda selkeät prosessikuvaukset ja vastuiden määrittelyt
- Luoda prosessikuvaukset yhtenäisillä käsitteillä
- Selvittää eri osapuolten tarpeet virkakortin elinkaaren hallinnasta yliopistoissa
- Tehdä ehdotus käytettävistä korteista, mahdollisista varmenteista ja muusta mahdollisesta teknologiasta sekä tarvittavista jatkotoimenpiteistä
- Priorisoida palvelut, joihin varmenteita käytetään
- Harkita lomakemallien luomista
- Huomioida toiminta palvelukeskusten avulla ja siihen liittyvät muutostilanteet
- Huomioida yliopistokohtainen sovellusvara ja jäsennellä käyttöönotto perusosaan sekä lisäosiin
- Luoda lokalisointivaraa prosessikuvauksiin
- Viestiä projektin keston aikana referenssiryhmälle ja -ryhmiltä
- Luoda toimintatapoja, jotka ovat välittömästi valmiita käyttöönotettavaksi
- Määritellä varmentaja, kortin toimittaja sekä korttien yksilöinti
- Tuottaa selkeä, joltain osin jopa yksityiskohtainen, ohje/suositus virkakorttien käyttöönotosta aikatauluineen Suomen yliopistoissa.

1.3 Projektiorganisaatio

Projektin on asettanut opetusministeriön OpIT-ryhmä. Projekti asetettiin 19.6.2007 ja sen ensimmäinen kokous oli 28.9.2007. OpIT yliopistoedustajat Kalervo Koskimies, Kari Välimäki ja Ilkka Siissalo, ja OPM:stä Irma Nieminen ja Esko Ala-Peijari muodostivat ohjausryhmän.

Projektipäällikkönä on toiminut IT-pääsihteeri Esko Ala-Peijari.

Projektiryhmään ovat kuuluneet seuraavat henkilöt:
Ilkka Siissalo, Helsingin yliopisto
Markku Kuula, Helsingin kauppakorkeakoulu
Antero Pajari, Lappeenrannan teknillinen yliopisto sekä yliopistojen IT-pääsihteeri
Andreas Pada, Åbo akademi
Jari Söderström, Taideteollinen korkeakoulu
Jukka Korhonen, Teknillinen korkeakoulu
Timo Korvola, Jyväskylän yliopisto
Mika Kauppi, Turun yliopisto
Christa Winqvist, Helsingin kauppakorkeakoulu
Mika Laaksonen, Helsingin kauppakorkeakoulu
Sami Saarikoski, OPM
Mikael Linden ja Urpo Kaila, tieteen tietotekniikan keskus CSC

Projektiryhmä on kokoontunut viisi kertaa. Tämän lisäksi projektin pienryhmät ovat kokoontuneet varsinaisten projektikokousten välillä.

Projekti on työnsä aikana kuullut asiantuntijoita, mm. Väestörekisterikeskuksen tuotepäällikkö Alf Karlssonia, sisäasianministeriön tietohallintojohtaja Kaarlo Korvolaa, Tampereen teknillisen yliopiston tietohallintojohtaja Jussi-Pekka Pispaa, Teknillisen korkeakoulun työasemaryhmästä vastaavaa Tommi Saranpäätä sekä Suomen Lyyra Oy:n edustajia.

1.4 Projektin hyödyt

Projektin tavoittelemat hyödyt määriteltiin seuraavasti:

- Projektin avulla voidaan parantaa tietoturvallisuutta ja voidaan toimia lainsäädännön ja muiden vaatimusten edellyttämällä tavalla. Elinkaaren hallinnan sekä priorisoinnin avulla käyttöönotosta tulee taloudellisempaa, tehokkaampaa ja ennustettavampaa.
- Projektin avulla luodaan edellytyksiä toteuttaa hyvää tietohallintatapaa ja luodaan mahdollisuuksia sähköiseen asiointiin.
- Yhtenäiset käytännöt palvelujen määrittelyssä helpottavat palveluiden ja teknologian käyttöönottoa.

1.5 Alustavan projektiraportin kommentointikierros

Projektiryhmä päätti pyytää kommentteja alustavalle projektiraportille yliopistojen IT- ja hallintojohtajilta sekä tietoturvapäälliköiltä. Kommentointipyyntö lähetettiin kyseisille tahoille sähköpostitse 19.2.2008.

Projekti sai runsaasti hyviä ja kriittisiäkin kommentteja raporttiluonnokseen. Raporttiluonnosta on kommentoitu sekä henkilökohtaisesti että IT-johtajien ja yliopistojen Secryhmän työvaliokunnan toimesta.

Projektiryhmä kiittää lämpimästi kommentoijia saaduista kommenteista, erityisesti seuraavia henkilöitä:

- Anna-Stina Nyby, Åbo Akademi
- Jussi-Pekka Pispa, Tampereen teknillinen yliopisto
- Stig-Göran Lindqvist, Åbo Akademi
- Seppo Visala, Tampereen yliopisto
- Asko Tontti, Teknillinen korkeakoulu
- Minna Manninen työryhmineen, Teknillinen korkeakoulu

Saadut kommentit on pyritty huomiomaan nyt käsillä olevassa raportissa, vaikka kommentit olivat osittain keskenään ristiriitaisia.

Kommentointikierroksen aikana on julkaistu uusi versio varmennekorttiohjelmistosta. Ohjelmiston käytettävyys ja toimivuus eri käyttöjärjestelmissä tulisi testata.

Valtiontalouden tarkastusvirasto on lisäksi julkaissut tarkastuskertomuksen (161/2008 Tunnistuspalveluiden kehittäminen ja käyttö julkisessa hallinnossa), jossa katsotaan, että Väestörekisterikeskuksen varmennetoiminta tulisi arvioida uudelleen tarvelähtöisesti ja että nykyisessä muodossaan Väestörekisterikeskuksen tarjoamille laatuvarmenteille on julkisessa hallinnossa vähän käyttöä. Joka tapauksessa Valtioneuvoston tietohallintoyksikön solmima puitesopimus virkakorteista tulisi kilpailuttaa uudelleen.

Kommenttikierroksessa nousi esiin lukuisten täsmennysehdotusten lisäksi mm. seuraavia asioita:

- Tarve huomioida myös muita todentamismenetelmiä laatuvarmenteiden rinnalla
- Yliopistojen oikeudellisen aseman muutoksen vaikutusten arviointi
- Tarve arvioida tarkemmin taloudelliset vaikutukset
- Tarve määritellä yhteisesti hyviä käytäntöjä logistisille ketjuille
- Joustavuustarpeen huomioiminen, koska suuri osa yliopiston henkilöstöä vaihtaa usein roolia
- Lukijoiden ja ohjelmistojen asennuksessa huomioitava, että merkittävä osa yliopistoissa käytössä olevista työasemista ei ole keskitetyn ylläpidon piirissä
- Palvelujen käytettävyyden parantaminen voi olla tärkeämpi tekijä uusissa todentamisratkaisuissa kuin pelkästään turvallisuusvaatimusten huomioiminen
- Useimmissa, mutta ei kaikissa yliopistoissa, käytetään tiettyihin palveluihin kuten pienmaksamiseen laajasti sähköisiä opiskelijakortteja.

Yleisvaikutelma kommenteista oli, että todentamisen kehittämistä pidetään tärkeänä ja ajankohtaisena asiana, mutta lisätietoa tarvitaan vielä, ennen kuin yhteisiä käyttöönottopäätöksiä uusista todentamisratkaisuista tehdään.

2 Taustaa

2.1 Varmennekortteihin liittyviä käsitteitä

Toimikorttia, joka sisältää varmenteen, kutsutaan varmennekortiksi.

Varmennetta voidaan käyttää henkilön tunnistamiseen tietoverkoissa. Varmenne perustuu julkisen avaimen infrastruktuuriin (public-key infrastructure, PKI) ja sisältää käyttäjän (varmenteenhaltijan) julkisen avaimen, jonka varmentaja on allekirjoittanut. Lisäksi varmennekortilla on käyttäjän yksityinen avain.

Varmennekortilla voidaan syrjäyttää salasanat tietojärjestelmiin kirjautumisessa, salata tiedostoja ja sähköpostiviestejä sekä laatia perinteiseen allekirjoitukseen rinnastuvia digitaalisia allekirjoituksia. Esimerkiksi poliisin kansalaiselle antama sähköinen henkilökortti on varmennekortti, mutta tässä dokumentissa ollaan kiinnostuneita työnantajan työntekijälle hankkimasta ns. organisaatiokortista, jota virastoissa kutsutaan myös virkakortiksi.

Varmenne sijaitsee varmennekortin sirulla ja sitä käytetään asettamalla kortti kortinlukijaan ja antamalla PIN-koodi. Varmennekirjautumisen käyttöönotto tietojärjestelmässä edellyttää muutoksia tietojärjestelmään, mutta itse korttia ei yleensä tarvitse muuttaa.

Tietojärjestelmään kirjautumisen lisäksi samalle kortille voidaan haluttaessa yhdistää myös muita toimintoja, mutta pääsääntöisesti se on tehtävä jo korttia määriteltäessä. Tällaisia ominaisuuksia on esimerkiksi visuaalinen tunnistaminen (kortinhaltijan nimi ja kuva painetaan muoviin), kulunhallinta (kortilla avataan yliopiston ovissa oleva sähkölukko) ja maksaminen (esim. henkilöstöravintolassa).

Lisätietoa varmennekortin käsitteistä on liitteessä A.

2.2 Vahva tunnistaminen ja todentaminen

Projekti perustuu oleellisesti vahvan tunnistamisen ja todentamisen tekniikoiden hyödyntämiseen.

Vahvan tunnistamisen tarpeellisuutta pohdittaessa sitä ei tule irrottaa kontekstistaan ja tarkastella yksittäisenä tavoitteena, vaan todentamisen vahvuus tulee suhteuttaa muihin käytettyihin turvamekanismeihin sekä suojeltavien kohteiden arvoon.

Vahvan todentamisen tarpeellisuus liittyy olennaisesti tiedon luokitteluun ja käsittelyyn (mm. HetiL 3§ kohta 2, julkisuuslaki (621/1999) ja julkisuusasetus (1030/1999)). Yliopistojen tulee itse täsmentää luetteloa luokiteltavista tiedoista ja suojattavista kohteista oman toimintansa osalta.

Myöskään arkistonmuodostussuunitelman (AMS) tai sähköisen arkistonmuodostussuunnitelman (eAMS) merkitystä ei kannata sivuuttaa.

Keskustelussa yliopistojen tietoturvapäällikköjen tapaamisessa Turussa 14.9.2007 todettiin, että projekti liittyy osin myös meneillään olevaan ValtIT:n tietoturvatasot-kärkihankkeeseen.

Jotta käyttöönottosuosituksesta ei tulisi liian häilyvä, tulee pyrkiä määrittelemään ja priorisoimaan vähimmäispalveluita sekä mahdollisia lisäpalveluita, joita voi käyttää varmennekorttien avulla. Käyttöönoton priorisointia on hyvä hahmottaa ns. Wardenin ympyrän avulla. Kun luokiteltua tietoa käsittelevät toiminnat on tunnistettu, voidaan siirtyä mahdollisiin lisäpalveluihin sekä määritellä niiden kohderyhmiä.

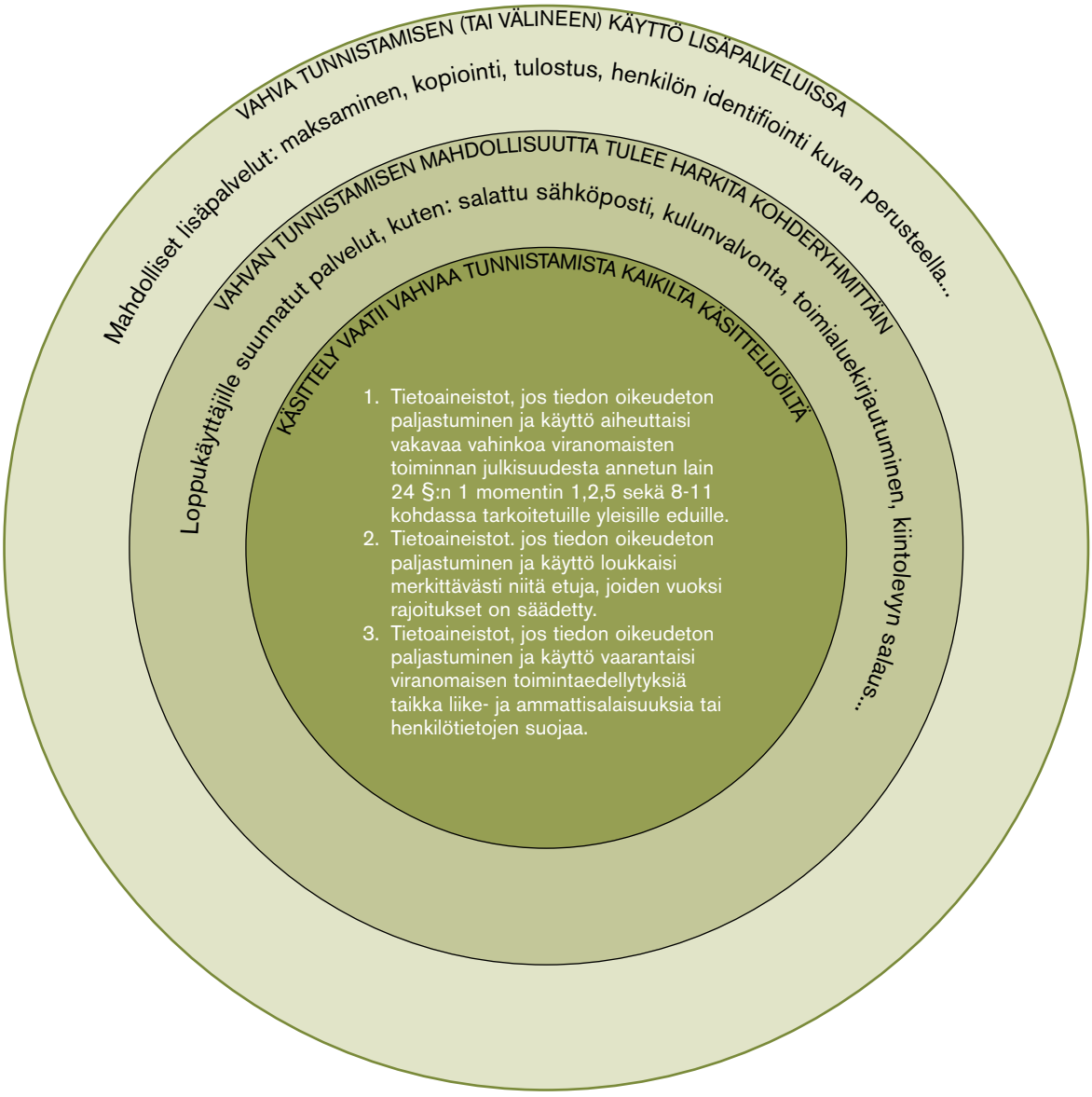
Teknisellä puolella tulee käsitellä esimerkinomaisesti käyttöönottoa muutaman palvelun osalta. Yksi näistä tulisi olla salattu sähköposti, koska sille tuntuu olevan tarvetta ainakin yliopistoissa.

Henkilötietoja sisältävien tietoaineistojen osalta tulee erityisesti huomioida pääkäytön ja ylläpitokäytön aiheuttamat riskit. Peruskäyttäjällä on yleensä pääsy ainoastaan omiin tietoihinsa, jolloin riskitkin ovat rajatumpia.

Tietojärjestelmä	Pääkäyttäjä, omistaja / luokittelija	Sisältääkö järjestelmä tai sen osa erityissuojattavaa tietoaineistoa? (perustelu)	Tietojärjestelmän sisältämän tiedon käsittelyluokka / turvallisuusluokka (KL IIV, Turvallisuusluokka IIV)	Vaatiiko käyttö vahvaa tunnistamista?	Vaatiiko pääkäyttö vahvaa tunnistamista?	Onko tietojärjestelmässä olevaa tietoa tarve salata: säilytettäessä / siirrettäessä / arkistoitaessa (mm. varmistukset)?
Sähköpostijärjestelmä	N.N.	Kyllä (SVTSL, 516/2004)	KL IV	Ei	Kyllä	Kyllä
Oodi	N.N.	Kyllä (HetiL, 523/1999)	KL II	Ei	Kyllä	Ei
Aktiivihakemisto	N.N.	Kyllä (HetiL, 523/1999)	KL IV	Ei	Kyllä	Ei
Tulostuspalvelu	N.N.	Ei	-	-	-	Ei
Tietojärjestelmien dokumentaatiopankki	N.N.	Kyllä (sisältää jopa salaista aineistoa: mm. palvelutunnusten salasanat, …)	Turvallisuusluokka III (SKVT, s.13)	Kyllä	Kyllä	Kyllä (SKVT, s. 13)
Organisaatio: Helsingin kauppakorkeakoulu, tietohallinto, tietoturvallisuus Hyväksyjä: Markku Kuula Hyväksytty: 26.10.2007						

Kuvio 1. Esimerkkilomake, jolla tunnistetaan suojattavat kohteet

Alla on mukaeltu Wardenin ympyrä, jossa tasot perustuvat käsiteltävän tiedon luokitteluun ja sekä henkilöryhmien toimenkuviin (pääsytasot: sähköinen ja fyysinen). Lisäpalveluita ei välttämättä tarvitse säädellä, mutta varsinkin ympyrän keskustaan kuuluvat palvelut tulee määritellä yhteisesti.



Kuvio 2. Vahva tunnistaminen/todentaminen ja Wardenin ympyrä

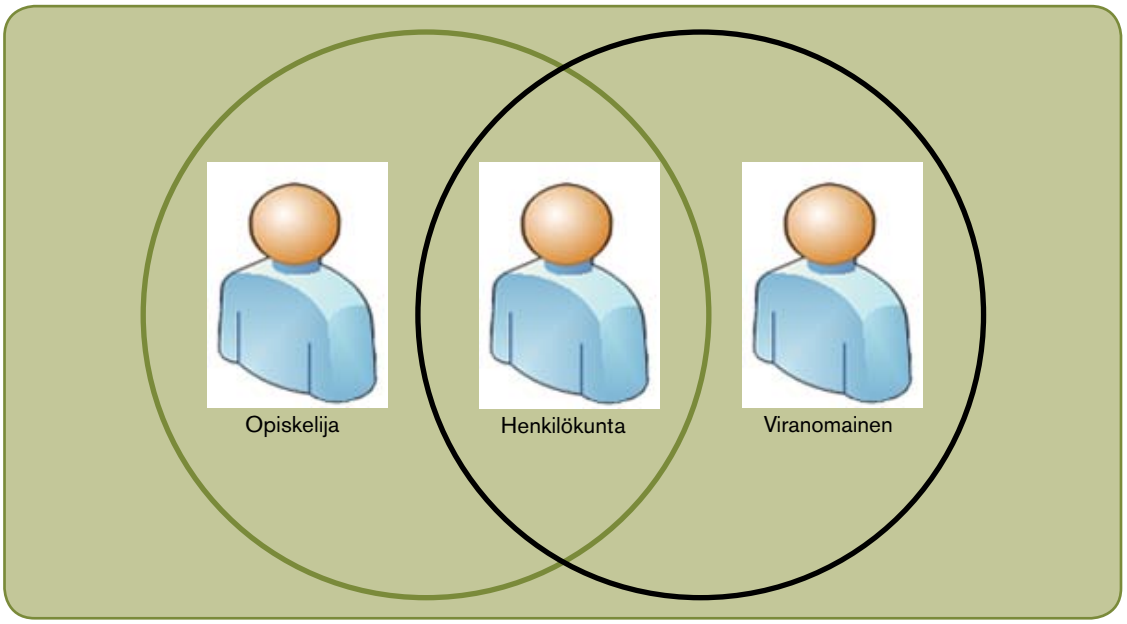
2.3 Todentaminen eri rooleissa

Yliopistoyhteisössä henkilö siirtyy usein roolista toiseen ja toimii useassa roolissa yhtä aikaa.

Opiskelija voi siirtyä esimerkiksi sivutoimiseksi tuntiopettajaksi tai tukihenkilöksi ja hallintotehtävissä toimiva henkilö voi myös olla sivutoiminen opiskelija.

Tietyt, yliopistoissa toimivat henkilöt voivat myös toimia selkeässä viranomaisroolissa.

Eri roolit tulee kuitenkin selkeästi eriyttää toisistaan. Viranomaistoiminta sekä palvelujen tuottaminen henkilöstöroolissa edellyttää korkeampaa tietoturvallisuutta kuin opiskelijan roolissa toimiminen.



Kuvio 3. Eri roolit yliopistoyhteisössä

Korkeimmat turvallisuusvaatimukset sekä lainsäädännön että riskienhallinnan kannalta kohdistuvat viranomaistoimintaan sekä kriittisiä palveluita tai henkilötietoja sisältävien tietojärjestelmien pää- tai ylläpitokäyttöön. Toisaalta yliopiston toiminnan kannalta on myös vähintään yhtä tärkeä turvata perustehtävien, tutkimuksen ja opetuksen turvallisuus suojaamalla luottamukselliset tutkimusaineistot.

Laissa sähköisistä allekirjoituksista (14/2003) todetaan, että jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen. Projektin aikana ainoa Suomessa laatuvarmenteita toimittava taho on Väestörekisterikeskus.

Suositus: Viranomaisroolissa tulee käyttää laatuvarmennetta.

Muissa tehtävissä todentamisen turvallisuusvaatimukset määräytyvät pääosin tietoaineiston luokituksen pohjalta sekä yliopiston riskienhallinnan ja tietoturvapolitiikan mukaan.

Todentamistekniikka tulee valita siten, että saavutetaan paras yhdistelmä kokonaisturvallisuuden, käyttömukavuuden sekä kustannusten kannalta. Todentamisen vahvuus on eräs keskeinen turvallisuuden osatekijä, mutta vasta kaikkien turvallisuusmekanismien, kuten esimerkiksi pääsynhallinnan, käyttäjähallinnon ja valvonnan, yhteisvaikutus kokonaisturvallisuuden tason.

Suositus: Vahvaa tunnistamista edellyttävissä työtehtävissä tulee käyttää kokonaisturvallisuuden kannalta parasta ja soveltuvinta tekniikkaa, joka voi olla laatuvarmenne, muu varmenne tai muu vahvan todentamisen menetelmä.

Opiskelijoille suunnatuissa palveluissa on useimmiten kyse laajasta käyttäjäkunnasta, jolla useimmiten ei ole pääsyä luottamukselliseen tietoon. Tämä raportti on rajannut ulos opiskelijoiden todentamismenetelmät ja keskittyy käsittelemään yliopistojen henkilökunnan ja mahdollisten viranomaistehtäviä hoitavien työntekijöiden tarvetta varmennekorttien käyttöön.

3 Tietoturvallisuus ja vaatimuksenmukaisuus

Tietoturvallisuusvaatimukset ovat tärkein syy ja peruste varmennekorttien käyttöönottoon yliopistoissa. Tietoturvallisuudella tarkoitetaan tässä sekä suojattavien järjestelmien ja palveluiden turvaamista että vaatimuksenmukaisuutta lakien, asetusten, määräysten ja sopimusten kanssa.

Palveluiden ja järjestelmien suojaaminen tulee perustua riskienarviointiin ja suojattavien kohteiden tunnistamiseen. Kriittiset järjestelmät ja palvelut, joiden toimivuus on tärkeää laajemmille käyttäjäryhmille, tulee luonnollisesti turvata paremmin kuin vähemmän kriittiset toiminnot, joilla on suppeampi käyttäjäkunta.

Turvamekanismien avulla suojattavien kohteiden luottamuksellisuus, eheys sekä käytettävyys voidaan saattaa riittävälle tasolle. Varmennekorttien avulla voidaan tietyissä tapauksissa parantaa henkilön tunnistamiseen sekä todentamiseen liittyviä mekanismeja. Pääsynhallinta on eräs tietoturvallisuuden keskeisimmistä turvamekanismeista.

Vaikka käyttäjätunnukseen liittyvät salasanat ovat yleisin tapa todentaa tietojärjestelmän käyttäjä, pidetään salasanoja kuitenkin heikkona todentamismenetelmänä. Vahvoina todennusmenetelminä voidaan pitää tunnistusavaimiin, varmenteisiin tai biometrisiin menetelmiin perustuvaa todennusta tai usean todennusmenetelmän yhdistelmää.

Suositus: Kriittisten tietojärjestelmien tärkeät toiminnot tulee turvata salasanoja luotettavammalla todentamismenetelmällä.

Salasanoja parempia todentamistekniikoita on useita: perinteiset varmennekorttipohjaiset tekniikat, ohjelmistovarmenneisiin tai eri viestintäkanavaa käyttäviin mobiilivarmenteisiin perustuvat tekniikat, kertakäyttösalasanat sekä erilaiset kertakäyttösalasanoja tuottavat laitteet, kuten RSA:n SecurID.

Salasanojen käyttöä ei yleisesti pidetä vahvan tunnistamisen menetelmänä. Tiettyjen palveluiden osalta palvelun tarjoaja tai tiedon omistaja, esimerkiksi Valtiokonttori, voi edellyttää käyttäjiltä vahvaa tunnistusta.

Turvallisuuden taso ei riipu yksinomaan salasanan tai varmenteen julkisen avaimen pituudesta, vaan laajasti myös muista tekijöistä, kuten tukitoimenpiteistä (esim. tilin lukitus liian monesta yrityksestä), käyttöohjeista, tuesta ja valvonnasta sekä turvallisuusjärjestelmän nopeudesta ja luotettavuudesta.

Tietojärjestelmään kirjautuessaan käyttäjät pyrkivät käyttämään sellaista menetelmää, joka on heille nopein ja helpoin. Jos kirjaantuminen varmennekorttia käyttäen on hidasta tai hankalaa, käyttäjät kirjautuvat mieluummin salasanalla, ellei niiden käyttöä ole estetty. Toisaalta lukuisten, vaikeiden ja useasti muutettavien salasanojen muistaminen on työlästä.

Suositus: Varmennekorttia tulee käyttää todentamiseen, kun vahva todentaminen on välttämätöntä ja tarkoituksenmukaista ja varmennekortti on paras turvatekniikka kyseisellä hetkellä.

Toinen merkittävä tekijä varmennekorttien käyttöönotossa on vaatimuksenmukaisuus lakien, asetusten, määräysten sekä sopimusten kanssa.

Julkisuuslain (621/1999) 12 §:ssä todetaan että viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä.

Tietoturvallisuudesta huolehtimisen vaatimus korostuu Sähköisen viestinnän tietosuojalaissa (516/2004).

Henkilötietolain (523/1999) 5-7 §:ssä sekä 9 §:ssä edellytetään erityistä huolellisuutta henkilötietojen käsittelyssä.

Laki sähköisestä allekirjoituksesta (14/2003) määrittelee virkavarmenteen käyttöä sähköisessä allekirjoituksessa.

Laki työntekijän yksityisyyden suojasta työelämässä (759/2004) asettaa myös epäsuorasti velvoitteen estää valtuuton pääsy henkilötietoihin.

Suositus: Keskeisten tietojärjestelmien ja henkilörekisterien pääkäyttö tai käyttö laajoin oikeuksin tulisi varmistaa vahvoilla turvallisuusmekanismeilla.

Projektin aikana valmisteilla oleva tietoturvallisuusasetus määrittelee turvallisuusluokkien lisäksi käsittelyluokat I – IV. Esimerkiksi käsittelyluokkaan III kuuluvat järjestelmät ja palvelut, jossa tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa yleisille ja yksityisille eduille. On luultavaa, että monet yliopistojen keskeiset tietojärjestelmät ja palvelut tulee luokitella käsittelyluokkaan III ja IV.

Pääosa yliopistoissa käsiteltävistä tiedoista julkista ja turvallisuusluokitellun tiedon osuus on melko pieni. Yliopiston turvallisuusjärjestelyt, valmiussuunnitelmat sekä tiettyjen tutkimushankkeisiin liittyvä tieto saattaa olla osittain turvallisuusluokiteltua luokissa I – III. Pääsääntöisesti yliopistoissa pyritään siihen, että tieto olisi mahdollisimman julkista

Yliopiston keskeisiä tietojärjestelmiä ovat esimerkiksi opiskelijarekisteri sekä yliopiston sähköpostijärjestelmät ja tallennusjärjestelmät, joihin voi sisältyä varmennus-, arkistointi-, levy- ja tiedostopalveluja. Näiden järjestelmien pääkäyttö tulisi toteuttaa vahvoilla turvallisuusmekanismeilla silloin kun se on teknisesti mahdollista ja taloudellisesti toteutettavissa kohtuullisin kustannuksin.

Vuoden 2008 aikana odotetaan tulevan voimaan uusi laki ja asetus, joilla oletetaan olevan vaikutusta varmenteiden käytön laajenemiseen. Esitys laiksi väestötietojärjestelmästä ja väestörekisterikeskuksen varmennepalveluista (HE 89/2008) on eduskuntakäsittelyssä.

Samoin valtioneuvoston asetusluonnos 2007 tietoturvallisuudesta ja hyvästä tiedonhallintatavasta valtionhallinnossa tulevat ennakkotietojen perusteella lisäämään varmenteiden käyttöä.

Taulukko 2 VAHTI-ohjeesta 12/06: Tunnistaminen julkishallinnon verkkopalveluissa

käyttäjäidentiteetti	**anonyymi**	**yksilöitävissä**		**kevyesti todennettu**		**vahvasti todennettu**	
Käyttäjän tunnistamistapa (todentamisen luotettavuus)	-	kevyt	vahva	kevyt	vahva	kevyt	vahva
Tietopalvelut ja tiedottaminen	x	x					
Asiakaspalaute ja kansalaisten osallistuminen	x	x					
Ei-luottamuksellinen vuorovaikutteinen asiointi		x		x			
Vireillepano	x	x		x	x		x
Luottamuksellinen vuorovaikutteinen asiointi					x		x
Tietojärjestelmien välinen tietojen vaihto							x
Viranomaispalvelut						x	x

3.1 Varmennepohjaisen todentamisen toteuttaminen

Varmennekortit eivät yksinään luo turvallisuutta, mutta voivat parhaimmillaan toimia turvallisuutta edistävinä komponentteina palveluissa.

Turvallisia IT-palveluita kehitettäessä kaikkien järjestelmän osien ja prosessien tulee olla määriteltyjä, dokumentoituja, ylläpidettyjä sekä koulutettuja ja tiedotettuja. Sovellettua lisätietoja tietoturvallisuudesta yleensä löytyy esimerkiksi valtionhallinnon VAHTI-ohjeista sekä alan kansainvälisistä suosituksista ja normeista.

Eräs tärkeä tekijä, joka tulee huomioida varmennekortteihin perustuvia palveluita kehitettäessä, on se, mitä lisäominaisuuksia korttiin liitetään.

Hyvä perussääntö on, että jos varmennekortti toimii lisäksi sekä kuvallisena henkilökorttina että kulunvalvontakorttina, tulee kulunvalvonnassa ottaa käyttöön PIN-kysely.

Ehdotus:

Otettaessa käyttöön uusia turvatekniikoita tulee varoa, ettei samalla luoda uusia riskejä. Tällainen tilanne syntyy esimerkiksi silloin, kun tiedon salaus voidaan purkaa vain varmennekortilla, joka on hukkunut, rikkoutunut tai ei ole muusta syystä käytettävissä. Ongelmaan ei ole olemassa yksinkertaisia ratkaisuja, mutta harkittavia keinoja ovat varaavaimen käyttö ja ongelmatilanteita torjuvat käytänteet.

4 Tuetut palvelut

Tässä kappaleessa kuvataan mihin palveluihin varmennekortteja voi hyödyntää yliopistoissa.
Raportin laatinut työryhmä on jäsentänyt palvelut

- vaadittuihin palveluihin, joissa salasanakirjautuminen tulisi ainakin korvata varmennekortilla tapahtuvalla kirjautumisella,
- suositeltaviin palveluihin, jossa varmennekorttien käyttöönotto olisi toivottavaa sekä
- lisäpalveluihin, joissa käyttöönottoa on syytä harkita tapauskohtaisesti.

Eri tahoilla voi olla erilaisia käsityksiä siitä, miten kypsää teknologiaa varmennekortit ja niitä hyödyntävät todentamistekniikat ovat. On olemassa melko varovaisia suhtautumisia mutta myös luottavaisesti varmennekorttien mahdollisuuksiin suhtautumista.

Varmennekorttien ja niitä edellyttävien palveluiden käyttöönotossa on useita ristikkäisiä riippuvuuksia. Jos palveluissa ei edellytetä varmennekortin käyttöä, on vaikeaa motivoida korttien käyttöönottoa. Toisaalta, jos varmennekortteja ei ole laajasti jaettuna, on uusien varmennekortteja edellyttävien palvelujen käyttöönotto työlästä.

Ehkä tärkein varmennekirjautumista edistävä tekijä on yksittäisen palvelun tuottajan päätös edellyttää varmennekortin käyttöä ainoana vaihtoehtona kirjautumisessa. Esimerkiksi Valtiokonttori on esittänyt, että Tahti- ja Heli-järjestelmien käytössä tulee siirtyä varmennekorttipohjaiseen kirjautumiseen. Lisäksi, mikäli Valtiokonttori ryhtyy edellyttämään varmennekorttien käyttöä huomattavasti laajempaa käyttäjäkuntaa koskettavien laskujenkäsittelyyn sekä matkustamiseen liittyvien Rondo- ja Travel-järjestelmien etäkäytössä yliopistojen luotettujen sisäverkkojen ulkopuolelta, voi korttien käyttäjäkunta laajeta huomattavasti. Kyseisiä palveluita saisi lähtökohtaisesti käyttää salasanatunnistuksella vain työnantajan ylläpitämistä järjestelmistä työnantajan ylläpitämästä verkosta. Rondo- ja Travel-järjestelmien turvallisuusvaatimukset edellyttävät kuitenkin tarkempaa arviointia kustannuksista ja hyödyistä.

Toinen erittäin keskeinen tekijä varmennekorttien käytön leviämisessä on se, onko käyttäjän mahdollista käyttää rinnakkain muita vaivattomampia tunnistautumistapoja, kuten salasanoja. Mikäli tunnistautuminen salasanoja käyttäen tietyssä palvelussa on sallittua, käyttäjien enemmistö todennäköisesti mukavuus- ja käytettävyyssyistä valitsee tämän tavan. Tunnistautuminen salasanojen avulla voi olla hyvä sallia, mikäli varmennekortilla tunnistautumisessa jostain syystä esiintyisi häiriöitä, mutta salasanojen käyttöön ei saisi olla mahdollista palata pelkästään mukavuussyistä.

Tietyt palvelut, kuten esimerkiksi työasemille kirjautuminen, ovat sellaisia, että varmennekorttien käyttöönoton kynnys on melko korkea. Työasemakirjautumisen luotettavuus ja nopeus vaikuttaa merkittävästi suuren käyttäjäjoukon jokapäiväisiin työtehtäviin. Häiriöt ja pidentyneet vasteajat voivat nopeasti johtaa hyvinkin kriittiseen palautteeseen.

Toisaalta työasemaverkkojen ja päätelaitteiden, kuten työasemien, turvallisuuden parantaminen on merkittävä haaste, varsinkin jos yhdellä tunnuksella on laajoja käyttöoikeuksia eikä pää- tai ylläpitokäyttöä suoriteta erillisellä tunnuksella.

Merkittävä varmennekorttien käyttöä vauhdittava tekijä voi olla salasanakirjautumiseen yhdistetty vaatimus salasanojen tiheästä vaihtamisesta. Tämä voi olla merkittävä edistävä tekijä varmennekorttien tai muiden kehittyneempien todentamistekniikoiden käyttöönotolle.

Varmennekortteja voisi myös hyödyntää esimerkiksi yhteydenpidossa kumppanien ja alihankkijoiden kanssa. Lisäksi varmenteiden käyttö saattaa helpottaa tunnusten ylläpitoa sekä esimerkiksi kustannusten jyvitystä.

Varmennekorttien avulla saattaa olla mahdollista saada entistä parempia edellytyksiä kehittää sähköistä asiointia ja siihen liittyviä digitaalisia allekirjoituksia ilman merkittäviä lisäkustannuksia. Digitaalisia allekirjoituksia voisi soveltaa esimerkiksi sähköisten tutkintotodistusten myöntämiseen.

Identiteetin hallinnan edelleen kehittäminen yliopistoissa on merkittävä kehittämiskohde. Toisaalta jo HSTYA-hankkeessa todettiin, että vahvan todentamisen väline ei sinänsä ratkaise käyttäjähallinnan ongelmia, vaan ne tulee ratkaista ennen kuin varmennekortit kannattaa ottaa käyttöön. Toisaalta organisaatiovarmenne tuo uuden tekijän organisaation identiteetinhallintaan ja luo myös uuden luottamusverkoston, jonka kautta on mahdollista tunnistaa sekä henkilö ja organisaatio.

VPN-etäkäyttöä on usea taho pitänyt palveluna, jossa varmennekorttien käyttöönoton aloittaminen voisi olla suotuisampaa kuin esimerkiksi kattava työasemille kirjautuminen kortin avulla. Itse laatuvarmennetta käytetäänkin vain allekirjoituksiin, ei tunnistamiseen.

Tarve tunnistaa ja todentaa entistä turvallisemmin sekä hallinnollinen että ylläpitotyöhön liittyvä etäkäyttö on koettu monella taholla tärkeäksi. Laatuvarmenteen käyttö etäkäytössä ei ole yleisesti turvallisuuden kannalta ehdoton vaatimus, vaan jokin muukin vahvan tunnistamisen menetelmä saattaa tulla kyseeseen. Saattaa kuitenkin joissain tapauksissa olla tarkoituksenmukaista ja taloudellista hyödyntää nimenomaisesti laatuvarmenteen sisältävää varmennekorttia VPN-etäkäyttöön.

Projekti tapasi työnsä aikana Teknillisen korkeakoulun työasemaylläpidosta vastaavan Tommi Saranpään ja hänen ryhmänsä ja sai näyttävän kuvauksen sekä demonstraation varmennekortin käytöstä mm. työasema- ja VPN-kirjautumiseen sekä Windows- että Linux-ympäristöissä.

4.1 Vaaditut palvelut

- Ulkoiset palvelut, joissa palvelun toimittaja edellyttää varmennekortin käyttöä (esim. valtionhallinnon yhteiset palvelut, kuten Valtiokonttorin Tahti-henkilöstötietojärjestelmä ja Heli-työpaikkahakujärjestelmä)
- Luottamuksellisten sähköpostien sähköinen allekirjoitus ja salaus
- Asiakirjojen sähköinen allekirjoitus ja salaus
- Viranomaistehtävät ja muu viranomaisten välinen valmius- ja varautumistoimintaan sekä muuhun turvallisuustoimenpiteisiin liittyvä luottamuksellinen viestintä.

4.2 Suositeltavat palvelut

- Etäylläpito varmennekortin tai muun vahvan todentamismenetelmän avulla
- Luottamuksellista tietoa sisältävät verkkopalvelut
- Opintohallintajärjestelmän pääkäyttö
- Talous- ja henkilöstöjärjestelmien hallinnollinen pääkäyttö
- Maksuliikenne
- Etäkäyttö (esimerkiksi VPN tai SSH)
- Pääsynhallinta työasemalle
- Muut todentamista vaativat palvelut (koska saattaa olla epätaloudellista tukea erikseen heikon todentamisen mekanismeja, jos samalla vahvalla todentamisella voi saada pääsyn myös heikkoa todentamista edellyttäville palveluille).

4.3 Lisäpalvelut

- Salasanojen vaihto
- Kulunvalvonta
- Varmennekäyttö älypuhelimessa
- Oman kirjaston kirjastokortti
- Kirjasto- ja bussikorttitoiminta
- Työajan seuranta.

4.4 Muut palvelut

Projekti on toimeksiantonsa mukaisesti selvittänyt mitä hyötyjä ja haittoja olisi yhdistää laatuvarmenteen sisältävä kortti henkilökohtaisia palveluita mahdollistavaan Lyyra-korttiin tai vastaavaan toiseen korttiin. Projekti on todennut mm. seuraavia hyötyjä ja haittoja:

- Ylioppilaskuntien liitto on korvaamassa perinteiset ylioppilaskortit Lyyra-toimikortilla. Sillä on jo olemassa laaja käyttäjäkunta ja infrastruktuuri ja sen kautta on pääsy palveluihin siellä missä kortti on otettu käyttöön. Sopimus on tehty jo yli 100.000 opiskelija Lyyra-kortin toimituksesta lähivuosina.
- Usean erillisen kortin käyttö on yleensä hankalaa, lompakoissa on jo nyt paljon erilaisia kortteja. Esimerkiksi TKK:n kampusalueella on useita erillisiä kortteja käytössä.
- Yliopistojen tulee arvioida mitä yhteisiä palveluja olisi käytettävissä, jolloin yhteinen korttistandardi toisi mukanaan etuja mm. päätelaite- ja ohjelmistopuolella, kuten yhteinen kulunvalvonta yhteisissä palveluissa, kuten kirjastopalvelut.
- Lyyra-korttijärjestelmään tehtyjä investointeja, kuten maksupäätteitä, on järkevää hyödyntää.
- Palvelu- ja varmennekorttien käyttöastetta ja markkinatilannetta tulevaisuudessa on vaikeaa ennustaa, tämän vuoksi suositusten tulee mahdollistaa päätöksenteon joustavuus tilanteen mukaan.
- Lyyra-korttijärjestelmän tietoturvallisuuden toteuttamisessa on ollut selkeästi parantamisen varaa, Lyyra-korttijärjestelmälle tulisikin suorittaa tietoturva-arviointeja yliopistojen Sec-ryhmän toimesta tai toimeksiannosta.

- Lyyra-kortti ei sisällä organisaatiovarmennetta, jota osa hallinnon palveluista edellyttää.
- Henkilökunnan ja opiskelijoiden korttien hallinnointiprosessi olisi joka tapauksessa erillinen johtuen erilaisista tarpeista. Henkilökuntakortin omistaa työnantaja.

Mikäli varmennepohjaista tunnistusta halutaan tulevaisuudessa laajentaa henkilökuntakäytön lisäksi myös opiskelijoille, lienee syytä harkita laatuvarmennetta edullisempien varmenteiden käyttöä. Varmenteita voisivat mahdollisesti tuottaa esimerkiksi yliopistot itse tai CSC- Tieteen tietotekniikan keskus Oy tai muu palvelukeskus.

Kulunvalvontajärjestelmässä käytettävän tunnisteen liittäminen varmennekortille on myös mahdollinen tapa vähentää käyttäjän hallussa olevien tunnisteiden lukumäärää. Kulunvalvontajärjestelmissä voidaan käyttää muun muassa 13,56 MHz:n taajuuteen ja RfID-tekniikkaan perustuvia passiivitunnisteita. Mikäli halutaan yhdistää kulunvalvontaominaisuus varmennekorttiin, tulee varmistua, että ainakin kulunvalvotuissa ulko-ovissa on PIN-kysely kytketty päälle. Tämä vaatimus korostuu, jos varmennekortti toimii samalla kuvallisena henkilökorttina, jolloin kadotetun kortin löytäjä saattaa päätellä kortinhaltijan pääsyoikeudet kiinteistön kulunvalvontajärjestelmässä. Lisäksi tulee huomioida, että mahdolliset muutostyöt kulunvalvontajärjestelmissä voivat aiheuttaa huomattavia kustannuksia.

Jos kulunvalvontajärjestelmän tunniste halutaan liittää varmennekortille, on syytä huomioida valtiovarainministeriön hanke erottaa työajanseurantaan ja kulunvalvontaan liittyvät järjestelmät toisistaan vuoden 2008 aikana turvallisuussyistä. Eriyttämisen vaikutukset varmennekorteille sisällytettäville palveluille on syytä arvioida erikseen.

Mikäli myös opiskelijat halutaan liittää laajemmin kulunvalvontajärjestelmän käyttäjiksi, saattaisi yhdistetyn Lyyra- ja kulunvalvontakortin käyttöönotto olla taloudellisesti mielekästä.

Projektiryhmä toteaa, että on syytä pitää selkeästi käsitteellisesti erillään yliopiston henkilökunnan käyttöön tarkoitettu varmennekortti kansalaisille tarkoitetusta kansalaisvarmenteesta, vaikkakin molemmat voivat perustua saman toimittajan teknologiaan.

5 Hallinnollinen toteutus

5.1 Varmennekorttiin liittyvien asioiden omistaja organisaatiossa

Organisaatiossa on oltava taho, joka vastaa varmennekortteihin liittyvistä asioista ja niiden kehittämisestä organisaatiossa. Vaihtoehtoina voidaan pitää ainakin

- Henkilöstöhallintoa, koska varmenne on palvelussuhteeseen liittyvä työväline ja siihen liittyvät prosessit liittyvät henkilöstöhallinnon prosesseihin
- Tietohallintoa sekä tilaajan että tuottajan roolissa, koska varmenne ja sen käyttö työasemissa on luonteeltaan tietotekninen asia.

Suositus: Varmennekorttiin liittyvät asiat virastossa omistaa henkilöstöhallinto, joka toimii tarpeen mukaan yhteistyössä tieto- ja tilahallinnon kanssa.

5.2 Päätös varmennetuen sisällyttämisestä yliopiston IT-infrastruktuuriin

Yliopiston ylin johto on vastuussa yliopiston tietoturvallisuudesta. Osana vastuutaan ylimmän johdon tehtävä on käynnistää toimenpiteet, joilla luodaan edellytykset varmenteiden käyttöön osana yliopiston tietoturvallisuuden toteuttamista.

Varmenteiden käytön edellytyksiin sisältyvät mm.

- Varmennekorttien elinkaaren hallintaan liittyvät prosessit ja niiden vastuuttaminen
- Varmennekorttien käyttöön työasemaympäristössä tarvittavat laitteistot, ohjelmistot sekä koulutus ja tuki
- Varmenteiden niveltäminen osaksi yliopiston käyttäjähallintoa, jos varmenteita halutaan käyttää myös yliopiston omiin tietojärjestelmiin kirjautumisessa.

5.3 Päätös varmennekirjautumisen edellyttämisestä yksittäisessä palvelussa

Päätöksen varmennekorttien käyttöönotosta tietyssä palvelussa tulisi perustua todentamistoiminnon riskianalyysiin, tietoturvavaatimuksiin sekä tilannekuvaan varmennekorttitekniikan käytettävyydestä sekä kustannuksista tiettynä ajanjaksona.

Koska tietoturvavaatimukset ovat yleisiä ja yliopistoilla on paljon samankaltaisia toimintoja ja järjestelmiä, olisi hyvä selvittää ja kokeilla varmennekorttien käyttöönottoa palvelukohtaisesti yhteistyössä.

Suositus: Päätöksen siitä, missä palvelussa varmennekirjautuminen vaaditaan, tekee palvelunomistaja yliopiston tietoturvapäällikköä kuultuaan. Päätöksen tulee perustua riskianalyysiin, tietoturvavaatimuksiin sekä tilannekuvaan varmennekorttitekniikan käytettävyydestä ja kustannuksista.

5.4 Päätös varmennekortin hankinnasta yksittäiselle virkamiehelle

Lähtökohtana voidaan pitää, että varmennekortti joko hankitaan kaikille tai määrätylle joukolle yliopiston työntekijöille tai yksikön päätöksellä yksittäisille henkilöille.

Jälkimmäisessä tapauksessa kortin tilaaminen perustuu tarveharkintaan ja työntekijän toimenkuvaan. Tarve kortin käyttöön määritellään tehtäväroolien perusteella.

Paras näkemys työntekijän toimenkuvasta on siinä yksikössä, jossa hän työskentelee (laitoksella tai vastaavassa yksikössä). Niinpä esitys yksittäisen varmennekortin hankinnasta on luontevaa tehdä yksikkötasolla. Päätöksen tekijänä voi olla tutkimusryhmän johtaja, laitosjohtaja, laboratorioinsinööri tai vastaava henkilö, jonka toimenkuvaan varmennekortin hankinnasta päättäminen kuluu.

Yliopisto voi tilata virkamiehelle varmennekortin ilman hänen suostumustaan, samalla tavalla jolla työnantaja järjestää työntekijälle muutkin työn tekemiseen tarvittavat henkilökohtaiset välineet, kuten puhelinliittymän, tietokoneen ja siihen käyttäjätunnukset. Virkamiehen informoiminen korttiin liittyvästä henkilötietojen käsittelystä voi tapahtua, kun kortti luovutetaan haltijalleen.

Suositus: Esitys yksittäisen virkavarmenteen hankkimisesta tehdään yksikkötasolla.

5.5 Rekisteröintipisteen sijoittaminen

Rekisteröintipiste (RA) on julkisen avaimen järjestelmän asiakasrajapinta: paikka, jossa varmennekortin saajan henkilöllisyys todennetaan, ja jossa varmistetaan, että varmenteeseen menevät henkilötiedot pitävät paikkansa. Rekisteröintipisteen sijoittelussa tulee huomioida, että rekisteröintipisteen henkilökunnan varahenkilöineen tulee saada huolellinen perehdytys tehtäviinsä.

Rekisteröintipisteen sijainnin tulee olla sellainen, että varmennekorttia hankkiva henkilö voi asioida siellä vaivatta. Jos yliopiston kampus on suuri tai hajanainen tai jos yliopistolla on sivutoimipisteitä, täytyy rekisteröintipisteitä järjestää useita.

Rekisteröintipisteeseen tarvitaan rekisteröinnin edellyttämät tietojärjestelmät, lukolliset säilytyspaikat noutamattomille varmennekorteille ja PIN-kuorille sekä valokuvan ottamiseen tarvittavat välineet, jos korttiin tulostetaan myös haltijansa valokuva.

Yliopistossa rekisteröintipisteen voi sijoittaa ainakin

- Tietohallinnon ATK-tukipisteeseen, jonka eduksi luetaan, että asiakas voi saada samasta pisteestä myös kortin työasemakirjautumiseen liittyvää opastusta ja neuvontaa.
- Virastomestareille/vahtimestareille tai muille avainhallinnasta vastaaville, joiden työtehtäviin kuuluu tyypillisesti avainten hallinta organisaatiossa. Rekisteröijän tehtävien antamista vahtimestareille tukee kortin mahdollinen käyttö kulunhallinnassa.
- Henkilöstöhallinnolle, joiden tehtäviin työsuhteeseen liittyvät prosessit kuuluvat organisaatiossa.

Suositus: Organisaatio arvioi oman toimintansa lähtökohdista, antaako rekisteröijän tehtävät ATK-tukipisteelle, virastomestareille vai henkilöstöhallinnolle. Arvioinnissa tulee huomioida ainakin olemassa oleva palvelupisteverkko, mahdollisen rekisteröintipisteen henkilöstön osaaminen ja rekisteröintipisteen tilat ja fyysinen turvallisuus.

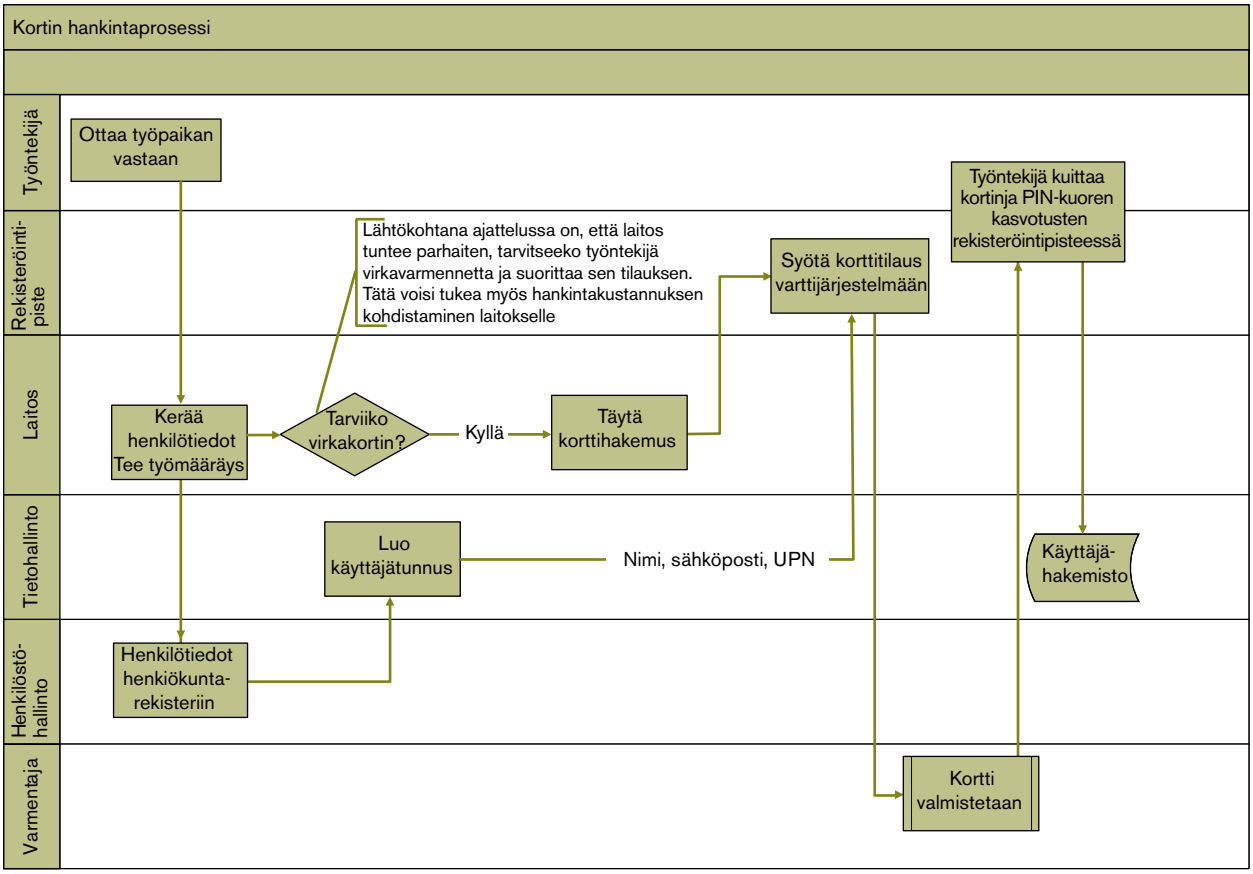
5.6 Prosessit

5.6.1 Varmennekortin tilaus- ja toimitusprosessi

Oheisessa prosessikaaviossa on esitetty varmennekortin tilaus- ja toimitusprosessi. Selvyyden vuoksi prosessikaavioon on sisällytetty myös työsuhteen alkamiseen liittyvinä tehtävinä henkilön tietojen kirjaaminen henkilökuntarekisteriin ja käyttäjän luominen käyttäjärekisteriin, koska näissä vaiheessa rekisteröitäviä henkilötietoja tarvitaan varmennepyynnön laatimiseen. Jos kyse ei ole varmenteen hankkimisesta uudelle työntekijälle, on nämä rutiinit tehty jo aikaisemmin.

Samassa yhteydessä, kun rekisteröijä ojentaa valmiin kortin työntekijälle,

- Rekisteröintivirkailija todentaa kortinhaltijan henkilöllisyyden poliisin myöntämästä tunnistusasiakirjasta, ottaa häneltä vastaanottokuittauksen ja tekee merkinnän käytetystä tunnistusasiakirjasta varmentajan vaatimusten mukaisesti.
- Rekisteröintivirkailija antaa kortinhaltijalle kortin käyttöön liittyvät säännöt ja ohjeet ja informoi häntä korttiin liittyvästä henkilötietojen käsittelystä (mm. varmenteen julkaisemisesta julkisessa varmennehakemistossa).
- Jos varmennekorttia on tarkoitus käyttää myös kulunhallintaan, rekisteröintivirkailija rekisteröi varmennekortin kulunhallintajärjestelmään kyseiselle henkilölle kuuluvaksi.
- Jos varmennekortilla on myös muita toiminnallisuuksia (esimerkiksi Suomen Lyyra Oy:n Lyyra-kortti), rekisteröintivirkailija tekee tarvittavat aktivointitoimenpiteet.



Kuvio 4. Kortin hankintaprosessi

Väestörekisterikeskuksesta on varmistettu, että loppukäyttäjän tarvitsee käydä rekisteröintipisteessä todentamassa henkilöllisyytensä vain yhden kerran, kun varmennekortti on valmistunut ja kuitattavissa. Varmennekortin tilaamista varten virkamiehen ei tarvitse pistäytyä rekisteröintipisteessä.

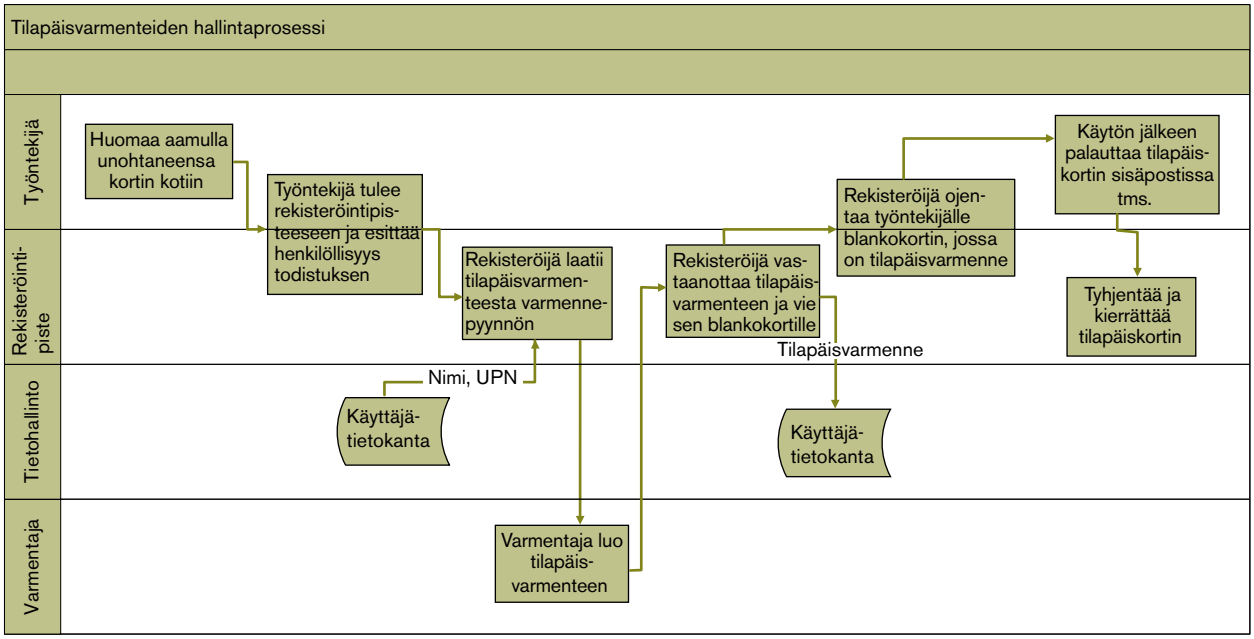
5.6.2 Varmennekortin uusimisen prosessi

Kortin uusimisprosessi on sama kuin edellisessä kohdassa esitetty kortin tilaus- ja toimitusprosessi.

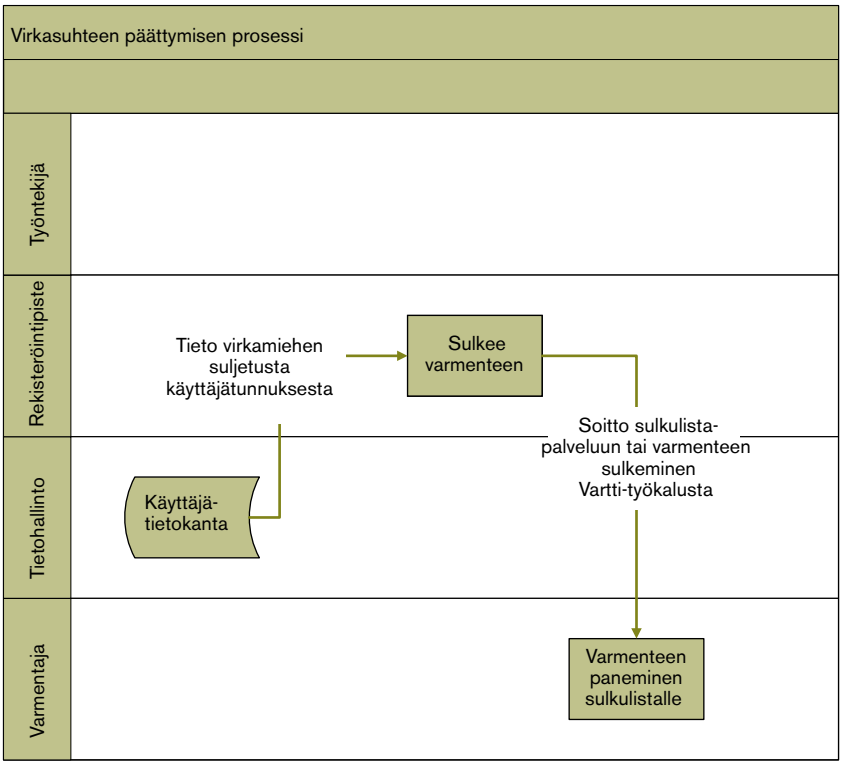
5.6.3 Tilapäiskorttiprosessi

Väestörekisterikeskuksen tuotevalikoimaan kuuluu myös tilapäiskortti ja -varmenne, joka luodaan rekisteröintipisteessä virkamiehen odottaessa, jos hän on unohtanut korttinsa, se on rikkoutunut tai ei muusta syystä ole käytettävissä.

Tilapäisvarmenne myönnetään VRK:n juurivarmentajan alta, mutta varmenne ei ole laatuvarmenne eikä sillä voi allekirjoittaa tai salata viestejä. Varmenne liitetään virkamiehen käyttäjätietoihin varmennehakemistossa. Kun tarve tilapäiskortille on päättynyt, kortti palautetaan rekisteröintipisteeseen uudelleenkäyttöä varten.



Kuvio 5. Kortin hallintaprosessi



Kuvio 6. Tilapäisvarmenteen päättymisprosessi

5.6.4 Virkasuhteen päättymiseen liittyvä prosessi

Virkasuhteen päättyessä tietohallinto, samalla kun sulkee virkamiehen työtehtäviin liittyvät käyttöoikeudet, pyytää rekisteröintipisteen virkailijaa sulkemaan virkamiehen virkavarmenteen. Sulkeminen voi tapahtua soittamalla sulkulistapalveluun tai käsin rekisteröintipisteen Väestörekisterikeskuksen tilauskäsittelyn Vartti-palvelun avulla.

6 Taloudelliset tekijät

Julkisen avaimen järjestelmän (PKI) ja siihen kytketyn toimikortin käyttöönotto organisaatiossa on edennyt melko verkkaisesti. Käyttöönotto on osoittautunut usein arvioitua kalliimmaksi. Kustannuslaskelmat ovat painottuneet kortin hankintakuluihin ja toimikortin lukijoihin. Varmenteiden integrointi tarjottaviin palveluihin sekä organisaation käyttäjähallintaan on osoittautunut usein paljon arvioitua kalliimmaksi. Yliopistojen ICT-ympäristö on perusperiaatteiltaan, mutta ei toteutusten osalta, melko yhtenäinen, joten yliopistojen yhteistyö on keskeisessä roolissa näiden kustannusten minimoinnissa vrt. Haka-luottamusverkosto.

Kustannukset voidaan ryhmitellä seuraavasti:

- Investointikustannukset, jotka syntyvät hankinnan yhteydessä, muodostuvat järjestelmäintegroinnista, korttikustannuksista, oheislaiteteknologiasta sekä käyttöönotto- ja koulutuskustannuksista
- Ylläpitokustannukset, joita ovat oman organisaation hallinnointi, tuki- ja koulutus, korttien vuosimaksut, teknologian ylläpito- ja tietoliikennekustannukset.

Laatuvarmenteen suuntaa antavat investointikustannukset henkilöä kohti ovat n. 100 €. Se jakaantuu melko tasan korttien hankintakulun, vaadittavan teknologian sekä käyttöönoton kesken. Laatuvarmennekorttien ylläpitokustannus vuodessa arvioidaan noin 20 %:ksi investointikustannuksesta eli noin 20 € henkilö/ vuosi, joka sisältää korttien uusimisen. Kokonaiskustannuksiin vaikuttaa olennaisesti miten kustannukset kohdistetaan, jaksotetaan ja arvostetaan.

Toimikorttien kokonaiskustannuksiin vaikuttavat merkittävästi myös seuraavat asiat:

- Mitä sovelluksia integroidaan palvelun piiriin ja millainen on sovellustoimittajien tarjoama tuki
- Valitaanko eri kortit eri palveluita varten vai monipalvelukortti
- Samalle varmennekortille liitetään muita palveluja kuten kuvallinen henkilökortti, kirjastokortti, avainkortti ja kulunvalvontakortti
- Tilattavien korttien kokonaismäärä vaikuttaa voimakkaasti yksikkökustannuksiin
- Käyttävätkö henkilökunta ja opiskelijat yhteensopivaa kortti- ja oheislaiteteknologiaa
- Toimikortin elinkaaren hallinnointiprosessi ja sen organisointi
- Kuinka yhtenäisiä yliopistojen todentamisjärjestelmät ovat.

Laatuvarmenteen investointikustannus vastaa henkilön alustavan arvion mukaan tunnin työaikakustannusta. Säästöt saadaan integroimalla mahdollisimman monta palvelua samalle kortille, jolloin voidaan yhtenäistää ja tehostaa aiemmat erillisten korttien ja avaimien hallintaprosessit. Hyötyjä saadaan myös siitä, että prosessin toiminta nopeutuu vahvan tunnistuksen avulla ja pakottaa käyttäjähallinnan virtaviivaistamiseen. Käyttäjien toiminta nopeutuu ja unohtuneiden salasanojen uusimisen aiheuttamat kustannukset jäävät pois. Toisaalta tulee huomioida koulutuksen ja viestinnän avulla, että käyttäjät eivät ohita suunniteltuja turvamekanismeja esimerkiksi kirjoittamalla PIN-koodiaan kortille.

Merkittävät hyödyt saavutetaan myös siitä, että kaikissa yliopistoissa on yhteensopivat tunnistustavat, jolloin korttikustannukset pienenevät, oheislaitekulut halpenevat, toimintaprosessit yhtenäistyvät, ylläpito voidaan ulkoistaa, käyttäjät voivat käyttää korttia esim. kaikissa yliopistokirjastoissa ja kahviloissa jne.

Tärkein hyöty on kuitenkin tietoturvallisuuden parantuminen, jonka taloudellinen arvo voi olla merkittävä.

Tuottavuusnäkökulmasta katsoen mahdollisimman integroitu monipalvelukortti yhtenäisellä ja suoraviivaisella hankinta- ja ylläpitoprosessilla kaikissa yliopistoissa vaikuttaa laskelmien valossa edullisimmalta ratkaisulta.

Toimikorttien ja varmenteiden kustannustehokasta käyttöönottoa puoltaisi yliopistojen tiivis yhteistyö ja mahdolliset yhteishankintasopimukset. Kokonaiskustannusten tarkentamiseksi ja mahdollisten piilokustannusten esille saamiseksi tulisi harkita ensin tarjouskilpailua ja käyttöönottoa yhdessä pilottiyliopistossa. Tämän jälkeen voitaisiin tarkemmin arvioida mahdollisen yhteishankkeen toteuttamista, sen kustannuksia ja vaikutuksia yliopiston kokonaisarkkitehtuuriin ja toimintakulttuuriin.

Mikäli pilotoinnin jälkeen päädytään yliopistojen yhteistyöhön toimikorttien hankinnassa, työryhmä suosittelee projektista kansallista hanketta, johon voisi hakea keskitettyä rahoitusta sekä VM/ValtIT:n että mahdollisesti ministeriön hankerahoituksesta.

Esimerkkejä kustannuksista: yksittäisen muovikortin kustannukset vaihtelevat 1 €-45 € riippuen kortista ja sen teknologiasta ja sisällöstä, taulukko 1.

korttityyppi	yksikkök. € (Alv 0%)	tekniikka
VRK-laatuvarmenne	21+ 6 e/vuosi	Kontaktisiru
Lyyra henkilökunta	25	RFID
Lyyra-opiskelija	15	RFID
VRK&Lyyra, yhdistelmä	40	Kontaktisiru+RFID
ID-kortti	5	Muovi+kuva
Avainkortti (sis RFID)	7	RFID
Kirjastokortti	1	Viivakoodi
Maksukortti	2	Mangneettinauha
Henkilökunnan työaika/h	60	

Seuraavassa on kustannus- ja hyötyalasyysi laatuvarmenteen käyttöönotosta ja ylläpidosta ja siihen liittyvistä kokonaiskustannuksista ja säästöistä. Kuten edellä on todettu, yksittäiseen kustannuserään vaikuttavat monet tekijät, joten laskelmaan vaikuttaa olennaisesti kuinka projekti toteutetaan ja millaiseen ympäristöön. Tämän esimerkin tarkoitus on antaa kokonaiskuva laatuvarmennekorttien kustannuksista ja säästöistä sekä niiden välisistä suhteista. Esimerkkilaskelma ei ota lainkaan kantaa tietoturvallisuuden paranemisesta

aiheutuviin kustannussäästöihin, vaikka se on varmenteiden käytön tärkein tavoite. Tässä laskelmassa keskitytään niihin tekijöihin, joilla on suora vaikutus kassavirtaan. Säästöistä suurimman osan arvioidaan tulevan työaikasäästöinä henkilöä kohti vuodessa. Kustannusarviossa esitetyt luvut on saatu tai arvioitu alan toimittajilta, tarjouspyynnöistä ja haastatteluista saaduista tiedoista. Hajonta on ollut suuri, joten esitetyt luvut ovat vain suuntaa antavia.

Laskelman mukaan laatuvarmennekortin investointikustannus on n. 100 € henkilöä kohti. Vastaavasti ylläpidosta aiheutuvat kulut vuodessa ovat yhteensä 22 € henkilöä kohti ja sen tuottamat työaikasäästöt ovat 47 € henkilöä kohti vuodessa. Näin ollen ylläpitokulujen ja säästöjen erotus on + 25 € vuodessa henkilöä kohti. Näillä lähtöarvoilla investointi maksaa itsensä takaisin n. 4 vuodessa. Laskelmassa kiinnittyy huomio siihen, että säästöt tulevat tehostuneista toimintaprosesseista, jossa toimikorttien hallinnointiprosessit ovat avainroolissa.

LAATUVARMENTEEN / MONIPALVELUKORTTI sisältää eri teknologiat	kust. €/ henkilö!	kust. €/ henkilö!
Investoinnit	ylläpito/v	investointi
Korttikustannukset (= siru + RFID+laatuvarmenne)		40
Perustamiskustannukset		
Korttimaksut		
Korttien painatus		
Mahdollisten lisävarmenteiden liittäminen korttiin		
Muu tekniikka		30
Lukijat		
Ohjelmistot		
PKI-työasemaohjelmistot		
Kortinlukijan ajurit		
Integrointi käyttäjähallintaan		
Kulunvalvontajärjestelmät		
Käyttöönotto		30
Projektikustannukset		
Konsultointi		
Koulutus		
Integrointi taustajärjestelmiin		
INVESTOINTIKULUT yht.		**100**
Ylläpitokustannukset (menot/v/henk.)	**yht. -22**	
Oman organisaation hallintokulut	-3	
Tuki ja koulutus	-2	
Korttien vuosimaksut	-6	
Ylläpitokustannukset (ohjelmistot ja laitteet)	-4	
Tietoliikennekustannukset	-1	
Korttien määräaikainen uusinta	-6	
Kustannusäästöt (tulot/v/henk.)	**yht. +47**	
Identiteetin hallintaprosessien uudistuminen (työ¬aika/henkilö) 20min/v	+20	
Käyttäjähallinnan virtaviivaistamisesta syntyvät säästöt	+7	
Toiminnan nopeutuminen vahvan tunnistuksen avulla (työaika/henkilö) 20min/v	+20	
Tietoturvallisuuden parantuminen tärkein säästö		
SÄÄSTÖ/VUOSI = tulot – menot	**==> +25**	

7 Tekniset ratkaisut

Tässä luvussa tehdään lyhyt katsaus varmennekortin käytön tekniikkaan ja tekniikan tämän hetken tukeen ja tasoon. Laajempi perehdytys on saatavilla mm. HSTYA- tutkimusraportista ”Julkisen avaimen järjestelmä, toimikortit ja niiden soveltaminen organisaatiossa.”[1]

Hankkeessa ei ollut mahdollisuuksia laajoihin kokeiluihin varmennekorttikirjautumisen toimivuudesta eri kortinlukijoiden, käyttöjärjestelmien ja sovellusten kanssa. Tämä luku perustuu lähinnä saatavilla olleeseen kirjalliseen dokumentaatioon, Väestörekisterikeskuksen kanssa käytyihin keskusteluihin ja haastatteluihin niissä hallinnonalan virastoissa, joissa varmennekorttikirjautumista käytetään tai kehitetään.

7.1 Varmenteen sisältö

Virkavarmenteet annetaan Väestörekisterikeskuksen varmentajan ”VRK CA for Qualified Certificates” alta. Tällä hetkellä voimassa on varmennepolitiikka ver 1.5 (OID: 1.2.246.517.1.10.3) ja varmennuskäytäntö ver 1.5 (OID: 1.2.246.517.1.10.3.1), jotka ovat saatavilla Väestörekisterikeskuksen WWW-sivuilta http://www.fineid.fi/

1 http://www.csc.fi/csc/julkaisut/oppaat

7.1.1 Varmenteen kentät

Varmennuskäytännön mukaan pakollisia varmenteen tietoja ovat

Pakollinen tieto	Selitys	Huomautus
2.5.4.5 (Serial Number)	Yksilöivä tunniste	Yksilöi varmenteen haltijan (seuraavat alaluvut)
SN (Surname)	Sukunimi	
G (Given name)	Etunimi	Etunimet
C (Country)	FI	

Varmennuskäytännön mukaan vapaaehtoisia tietoja ovat

Vapaaehtoinen tieto	Selitys	Huomautus
O (Organization)	Organisaation nimi	VRK:n suullisten ohjeiden ja VRK:n FINEID S2-määrityksen mukaan pakollinen tieto. Kielestä ei ole ohjeistusta, lienee tarkoituksenmukaista käyttää yliopiston ensimmäistä virallista kieltä.
OU (OrganizationalUnit)	Organisaatioyksikkö	Emme suosittele käytettäväksi, jotta yliopistojen organisaatiouudistuksista ei seuraa kaikkien varmenteiden uusiminen.
Title	Nimike	Tehtävänimike. Emme suosittele käytettäväksi, jotta työtehtävien muutoksesta ei seuraa varmenteen uusiminen
Email address	Sähköpostiosoite	Tarvitaan turvasähköpostissa. Suosittelemme käytettäväksi käyttäjän yksilöimisessä. Sijoitetaan varmenteen Subject Alternative Name -kenttään.

Lisäksi varmenteessa voi varmenteen haltijasta olla ainakin seuraavat tiedot, vaikka varmennekäytäntö ei mainitse asiasta:

Other Name: User Principal Name	Windows-toimialueen käyttäjätunnus	username@domain. Pakollinen Windows-toimialueen kirjautumisessa. Väestörekisterikeskuksen toteutuksessa tällä hetkellä sama kuin sähköpostiosoite, mutta voidaan toimialueessa kuvata myös johonkin toiseen käyttäjätunnukseen (UPN suffix).

Liitteenä on esimerkki VRK:n organisaatiovarmenteesta.

On hyvä huomioida, että jos joku varmenteessa oleva tieto muuttuu kesken varmenteen voimassaoloajan, tulee yliopiston asettaa varmenne sulkulistalle ja hankkia työntekijälle uusi kortti ja varmenne. Väestörekisterikeskus perii uudesta varmenteesta normaalin hinnaston mukaisen maksun. Muuttuvia tietoja voivat esimerkiksi olla

- Nimi (henkilön sukunimi muuttuu)
- Sähköpostiosoite (henkilön nimi muuttuu tai yliopistoon tulee täysikaima ja yliopiston käytäntönä on rikkoa kaimoista ensimmäisen sähköpostiosoite. Esimerkiksi esko.esimerkki@yliopisto.fi muutetaan muotoon esko.k.esimerkki@yliopisto.fi)
- Yliopiston nimi (yhdistymiset, nimenmuutokset)
- Organisaatioyksikön nimi (organisaatiomuutokset)
- Tehtävänimike (työtehtävien vaihtuminen).

7.1.2 Varmenne ja yliopiston käyttäjähallinto

Jotta varmenne saadaan nivellettyä sulavasti yliopiston sisäiseen käyttäjähallintoon, on varmenteenhaltijan yksilöivän tunnisteen huomioiminen keskeistä. Tavoiteltavaa on, että varmenteesta löytyy sellainen varmenteenhaltijan yksilöivä tunniste, jolla on merkitys yliopiston käyttäjähallinnossa. Tällöin varmenne voidaan yhdistää oikeaan käyttäjään ja hänen käyttövaltuuksiinsa yliopiston sisäisessä käyttäjähallinnossa (esim. LDAP-hakemistossa) automaattisesti, eikä manuaalista toimenpidettä tarvita.

Yhdistämisalgoritmi on yksinkertainen:

1. Poimi varmenteesta varmenteenhaltijan yksilöivä tunniste.
2. Tee LDAP-haku yksilöivän tunnisteen perusteella
   a. jos osumia tulee nolla, ei mainittua käyttäjää löydy yliopistosta. Todennäköisesti tilausprosessissa on syntynyt virhe. Lopeta tähän.
3. Kirjoita varmenne LDAP-hakemistoon kyseisen käyttäjän objektiin userCertificate-attribuuttiin (katso funetEduPerson 2.0).

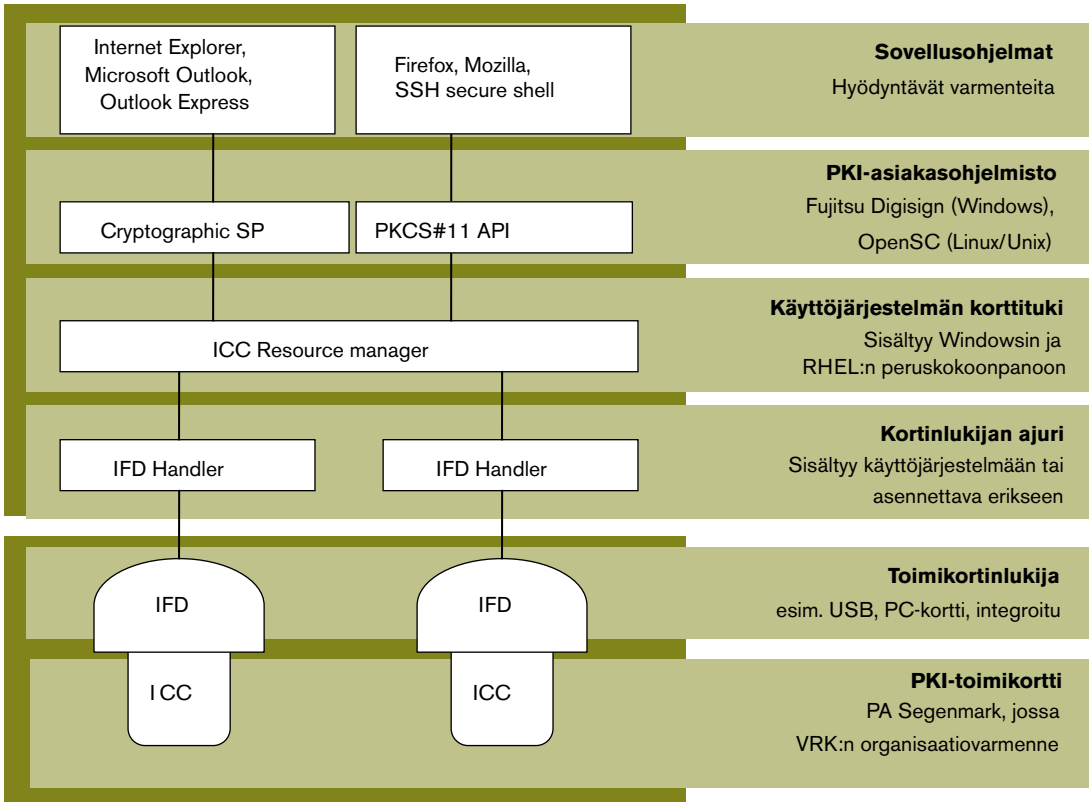
Yhdistämisalgoritmi voidaan suorittaa kolmessa vaihtoehtoisessa vaiheessa. Vaihetta on seuraavassa listattu siinä järjestyksessä, jossa työryhmä niitä suosittelee:

1. Rekisteröintipisteessä, kun varmenteenhaltija kuittaa varmennekorttiaan. Yhdistäminen tapahtuu niin, että rekisteröintipisteen virkailija käyttää kortin kortinlukijassa, joka lukee kortin varmenteen (tähän ei tarvita PIN-koodia) ja käynnistää Yhdistämisalgoritmin. Järjestelyn etuna on, että samalla tulee testatuksi kortin karkea toimivuus. Lisäksi rekisteröintipisteen virkailija tietää, miten mahdolliset Yhdistämisalgoritmin ajossa syntyneet ongelmat ratkaistaan.
2. Sillä hetkellä, kun varmenteen saanut työntekijä ensimmäistä kertaa kirjautuu kortillaan tietojärjestelmään. Työntekijä voi esimerkiksi saada rekisteröintipisteestä kirjallisen ohjeen, jossa hänen kehoitetaan aktivoimaan saamansa varmenne itsepalveluna menemällä osoitteeseen https://www.yliopisto.fi/tietohallinto/varmenne.
3. Synkronointiajossa, jossa yliopisto noutaa uusia varmenteita Väestörekisterikeskuksen tietojärjestelmistä. Synkronointiajo voisi tapahtua esimerkiksi öisin. Synkronointiajon järkevä toteuttaminen edellyttää, että Väestörekisterikeskus tarjoaa rajapinnan, jonka kautta yliopisto saa tiedon yliopiston virkamiehille myönnetyistä uusista varmenteista.

Neljäntenä vaihtoehtona voidaan pitää sitä, että virkavarmennetta ei lainkaan tallenneta organisaation LDAP-hakemistoon, vaan Yhdistämisalgoritmi ajetaan dynaamisesti joka kerta, kun käyttäjä kirjautuu. Vaihtoehto on periaatteessa toimiva, mutta eri palvelintuotteiden tuki sille on epäselvä.

7.1.3 Yksilöivä tunniste Väestörekisterikeskuksen varmenteessa

Väestörekisterikeskuksen organisaatiovarmenteissa sähköpostiosoite on ainoa kenttä, joka soveltuu varmenteenhaltijan yksilöimiseen organisaation sisäisessä käyttäjähallinnossa. Tällä hetkellä User Principal Name (UPN) -kenttä sisältää myös sähköpostiosoitteen. Kun Väestörekisterikeskus on myöntänyt yliopiston työntekijälle uuden varmenteen, tulee yliopiston ajaa Yhdistämisalgoritmi, jotta varmenteenhaltija jatkossa yhdistetään oikeisiin käyttövaltuuksiin. Windows-työasemakirjautumisessa käytetään aina UPN-arvoa, joka yhdistetään oikeaan tilin Windowsin omilla välineillä (UPN suffix).



Kuvio 7. Esimerkki työaseman varmennekortteja tukevasta ohjelmistoarkkitehtuurista

Sähköpostiosoitteen käytössä yksilöivänä tunnisteena yliopiston tulee varmistaa Yhdistämisalgoritmin oikea toiminta myös tilanteessa, jossa

- Taloon tulee täyskaima, joka johtaa olemassa olevan työntekijän sähköpostiosoitteen rikkomiseen ja varmenteen panemiseen sulkulistalle
- Sähköpostiosoitteen haltija poistuu talosta, ja karenssiajan jälkeen osoite kierrätetään eri henkilölle.

Myös varmenteenhaltijan sarjanumero on luonteeltaan varmenteenhaltijan yksilöivä tunniste, mutta yliopisto ei voi vaikuttaa sen määräytymiseen. Sarjanumeron generoi Väestörekisterikeskus (Vartti-työkalu). Jos yliopisto haluaa, että samalle henkilölle tulevaan uuteen varmenteeseen tulee sama sarjanumero, tulee yliopiston pyytää sitä varmennetta tilattaessa (Vartti-työkalussa).

7.2 Varmennekortti ja työaseman ohjelmistoarkkitehtuuri

Toimikortinlukijan sisältävän työaseman ohjelmistoarkkitehtuuriksi on Windows-ympäristössä vakiintunut melko raskas ja monimutkainen PC/SC[2], joka on kuvattu alla. PKI-toimikortin, kuten Väestörekisterikeskuksen organisaatiokortin, käyttämiseen tarvitaan erityistä PKI-asiakasohjelmistoa.

2 **http://www.pcscworkgroup.com/**

Windows-käyttöjärjestelmissä toimikorttituki on ollut mukana Windows 2000:sta alkaen, ja se tunnistaa automaattisesti yleisimmät kortinlukijat. Unix- ja Linux-ympäristössä tuki on heikompi. Teknillisen korkeakoulun ATK-keskuksessa unix-ryhmä on HSTYA-projektin puitteissa osallistunut OpenSC-ohjelmiston kehittämiseen. Tämä toimikorttijärjestelmä oli käytössä useamman vuoden atk-luokissa opiskelijoilla ja pienellä osalla henkilökuntaa. Työasemien toimikorttituki ajettiin kuitenkin lopulta alas, koska toimikorttien käyttäminen ei kiinnostanut käyttäjiä.

Nykyisen IT-palvelukeskuksen (entinen atk-keskus) työasemaryhmä on rakentanut Red Hat Enterprise Linux (RHEL) 5.1 -työasemakonseptiinsa toimikorttitukea.

Helsingin yliopiston tietotekniikkaosasto on kokeillut varmennekortteja Ubuntu Linux-työasemissa[3].

Saatavilla on lukuisia eri toimikortinlukijamalleja, jotka liitetään työasemaan USB-liitännän tai PC-kortin välityksellä tai integroidaan osaksi työaseman kotelointia tai näppäimistöä. Esimerkiksi Hansel oy:llä on puitesopimus Dellin näppäimistöön integroidusta toimikortinlukijasta, jota on hyödynnetty sekä TKK:lla että OPM:ssä. Windows ja RHEL tunnistavat Dellin näppäimistölukijan automaattisesti, ilman erillistä kortinlukija-ajurin asentamista.

Merkillepantavaa on, että PDA-laitteisiin ja matkapuhelimiin ei tiettävästi ole kaupallisesti saatavilla toimikortinlukijaa. Tämä käytännössä estää virkavarmenteeseen tukeutuvan kirjautumisen matkapuhelimesta ja PDA-laitteesta.

Varmennekorttien käyttäminen edellyttää lisäksi PKI-asiakasohjelmiston asentamista työasemaan. PKI-asiakasohjelmisto toteuttaa sovellusohjelmille rajapinnan, jonka kautta ne voivat käyttää toimikorttia. Microsoftin sovellukset (IE, Outlook, Windows logon) käyttävät Cryptographic Service Provideria (CryptoAPI, CSP) ja useimmat muut (mm. Firefox, Mozilla, Thunderbird) PKCS#11-standardin mukaista rajapintaa.

Väestörekisterikeskuksen organisaatiokorttien toimittaja kilpailutettiin syksyllä 2007, jolloin Gemalton (Setecin) tilalle valittiin PA Segenmark. Samalla Setecin PKI-asiakasohjelmiston (SetWeb) syrjäytti Fujitsun Digisign, joka Väestörekisterikeskuksen mukaan tukee Windows 2000/XP/2003 Server/Vista, SUSE Linux Enterprise Desktop 10.3 SP1, Red Hat Enterprise Linux 5 ja Ubuntu 7.10 sekä 8.04 -käyttöjärjestelmiä. Digisign on saatavilla Väestörekisterikeskuksen WWW-sivuilta. Fujitsun Digisign tukee myös vanhoja Setecin kortteja, joten jos yliopistossa on sekä vanhoja Setecin kortteja että PA Segenmarkin kortteja, riittää että työasemiin asennetaan Digisign. Tätä kirjoitettaessa PA Segenmarkin kortteja ei vielä ole saatavilla.

Työryhmä suosittelee, että PA Segenmarkin varmennekortteja ja niiden yhteentoimivuutta Digisign-asiakasohjelmiston, eri kortinlukijoiden ja sovellusten kanssa testataan.

Teknillisen korkeakoulun ATK-keskus on käyttänyt RHEL-ympäristössä avoimen lähdekoodin OpenSC-kirjastoa[4]. OpenSC-projektin mukaan[5] OpenSC tukee myös muita Linux-variantteja, Solarista, Mac OS X:ää sekä Windowsia, mutta emme ole tietoisia, että niitä olisi yliopistoissa käytetty. OpenSC-kirjaston tuesta PA Segenmarkin toimittamille varmennekorteille ei ole kokemusta.

---

3 **http://www.helsinki.fi/~aulaskar/tietos/korttitunnistus/kortti.html**
4 **http://www.opensc-project.org/**
5 **http://www.opensc-project.org/opensc/wiki/OverView**

7.3 Varmennekirjautumisen hyödyntäminen sovelluksissa

Varmennekirjautumista voidaan hyödyntää PKCS#11- tai CSP-rajapinnan kautta, jos työasemaan on asennettu edellisessä kappaleessa esitetyt ohjelmistot. Tässä kappaleessa kuvataan lyhyesti niitä asiakasohjelmisto- ja palvelinpään muutoksia, mitä kirjautuminen eri järjestelmissä edellyttää.

7.3.1 Windows-toimialueen kirjautuminen

Windows-käyttöjärjestelmä on tukenut toimikorttikirjautumista Windows 2000:sta alkaen. Kirjautuminen on mahdollista suorittaa myös VPN-yhteyden yli.

Toimikorttikirjautuminen edellyttää, että varmenteen sisällössä on oikeanlaiset kentät. Muun muassa Subject Alternative Name -kentässä on oltava käyttäjän UPN-tunniste (User Principal Name) ja varmenteen käyttötarkoitukset -kentässä (Extended key usage) SmartCardLogon -arvo. Tällainen varmenne voidaan toteuttaa

1. niin, että mainitut arvot tulevat suoraan Väestörekisterikeskuksen antamaan organisaatiovarmenteeseen, ja konfiguroimalla Windows Domain Controller luottamaan niihin, tai
2. pystyttämällä yliopistolle oma varmentaja (CA) esimerkiksi Microsoftin tarjoamilla välineillä ja käyttämällä varmentajaa erillisten, yliopiston itse allekirjoittamien kirjautumisvarmenteiden lisäämiseen Väestörekisterikeskuksen organisaatiokorteille. Väestörekisterikeskuksen kortilla on jonkun verran tyhjää tilaa tällaisia varmenteita varten.

Työryhmä suosittelee vaihtoehtoa 1.

Väestörekisterikeskuksen ja Microsoftin tekemä tiivis mutta kattava ohje Windows-toimialueen varmennekirjautumisesta on saatavilla VRK:n sivuilta[6]. Toimikorttikirjautumista on käsitelty tarkemmin Microsoftin tekemässä ohjeessa[7].

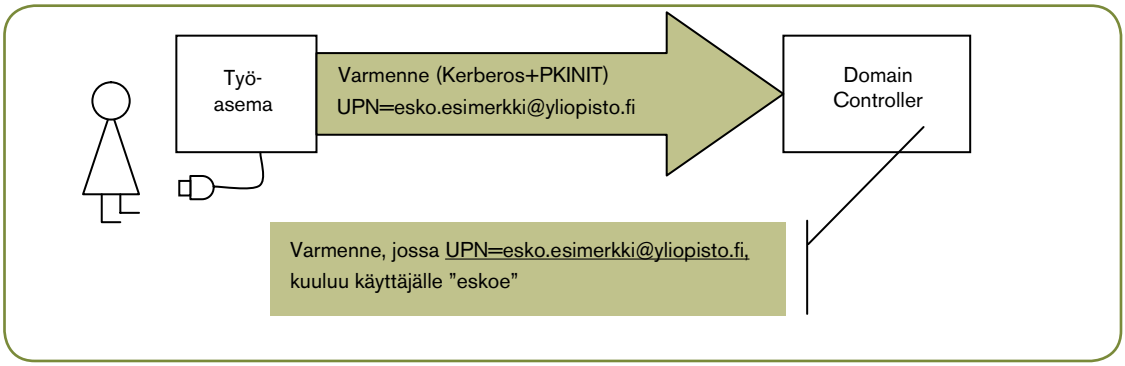
---

6 **Kolmannen osapuolen sisäänkirjautumisvarmenteet Windows 2003/XP ympäristössä http://www.fineid.fi/vrk/fineid/files.nsf/files/0F27CDE81545A5E7C225708A00467D71/$file/logon_org.pdf**

7 **http://support.microsoft.com/kb/281245**

Kuvio 8. Varmenteen UPN-arvon kuvaaminen toimialueen käyttäjätunnukseen

On vielä hyvä huomata, että varmenteen UPN-arvon ei tarvitse välttämättä olla sama, jolla käyttäjä tunnetaan toimialueessa, vaan toimialue voi kuvata varmenteen UPN-arvon toimialueessa käytettyyn UPN-arvoon UPN Suffix –toiminnon avulla. Esimerkissä (Kuv) varmenne, jossa UPN=esko.esimerkki@yliopisto.fi, on kuvattu käyttäjästä toimialueessa käytettyyn käyttäjätunnukseen ”eskoe”. Tästä on hyötyä, jos yliopistossa on useita Windows-toimialueita, johon samalla varmenteella halutaan kirjautua, tai jos varmenteenhaltijan käyttäjätunnuksen ei haluta näkyvän julkisessa hakemistossa olevassa varmenteessa.



Kuvio 8. Windows-työasemakirjautuminen

7.3.2 Unix-työaseman kirjautuminen

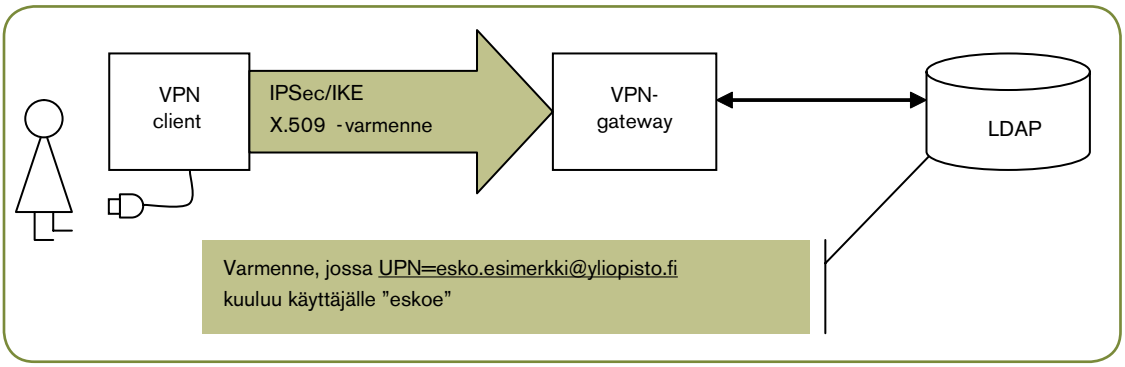
Teknillisen korkeakoulu on kehittänyt ATK-keskuksen RHEL-työasemiin toimikorttikirjautumisen, joka käyttää Kerberos-protokollaa Windows-toimialueen Domain Controlleria vasten tapahtuvassa kirjautumisessa. TKK:n toteutuksen komponentit on esitetty alla.

Komponentti	Merkitys
Dell-näppäimistöön integroitu kortinlukija	
RHEL-käyttöjärjestelmä	Distribuutio sisältää kortinlukijan ajurin ja käyttöjärjestelmän korttituen (PC/SC)
OpenSC http://www.opensc-project.org/opensc/	Toteuttaa PKCS#11-rajapinnan
PAM_PKCS11 http://www.opensc-project.org/pam_pkcs11/	Poimii kortilta varmenteen UPN-arvon ja tekee kyselyn LDAP-hakemistoon saadakseen sitä vastaavan SAMAccountNamen, jonka se ojentaa PKINIT:lle
Heimdahl PKINIT http://people.su.se/~lha/patches/heimdal/pkinit/	Toteuttaa varmenneautentikoinnin Kerberos-kirjautumiseen
SAMBA	Toteuttaa LDAP-haun AD:tä vasten

Teknillisessä korkeakoulussa RHEL-työasemien varmennekirjautuminen rakentuu Kerberoksen ja Active Directoryn ympärille. Turvapostia, WWW-kirjautumista ja SSH Secure Shell -kirjautumista ei ole RHEL-työasemissa testattu, suunnitelmia niiden rakentamisesta Kerberoksen varaan on TKK:lla olemassa. OpenSC:n tarjoaman PKCS#11-rajapinnan pitäisi kuitenkin mahdollistaa varmennekortin käyttö myös WWW-selaimessa ja sähköpostiasiakasohjelmistossa.

7.3.3 VPN-etäyhteydet

IPSec/IKE-pohjaiset VPN-etäyhteydet ovat yksi varmenteella tapahtuvan vahvan autentikoinnin mahdollisista käyttökohteista. Useat VPN-asiakasohjelmistot tukevat varmenteeseen perustuvaa autentikointia PKCS#11 -rajapinnan kautta.

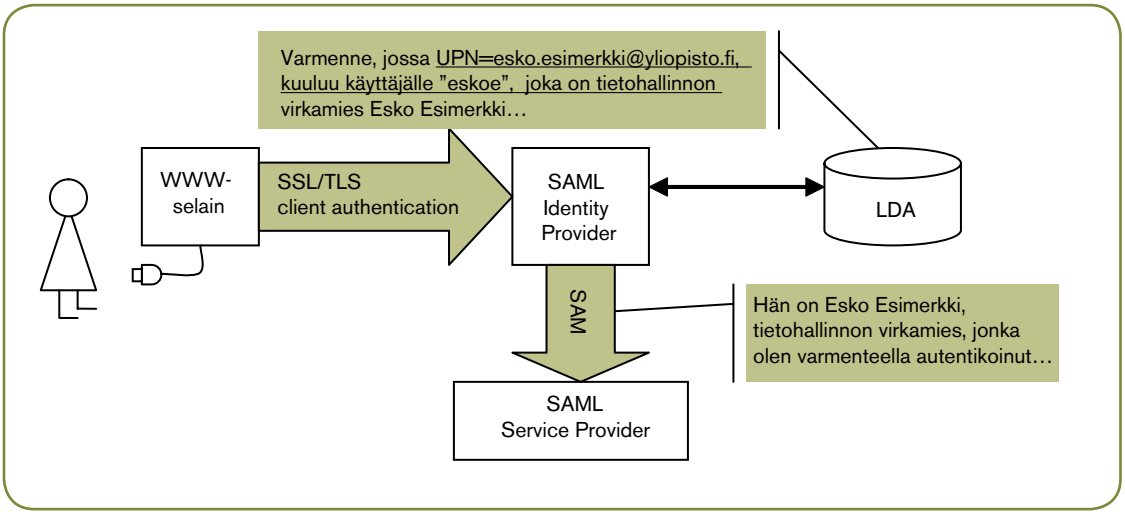


Kuvio 9. Varmennekirjautuminen VPN-yhteyksissä

7.3.4 WWW-kirjautuminen

Microsoftin Internet Explorer -selain osaa hyödyntää varmennetta CSP-rajapinnan kautta. Mozilla-pohjaiset selaimet voivat käyttää varmennetta PKCS#11-rajapinnan kautta.

WWW-ympäristön protokollissa varmennekirjautuminen tapahtuu lähes poikkeuksetta SSL-protokollan tasolla, jolloin aloitteen varmennekirjautumisesta tekee WWW-palvelin. Sekä Apache että IIS on konfiguroitavissa varmennekirjautumiseen.



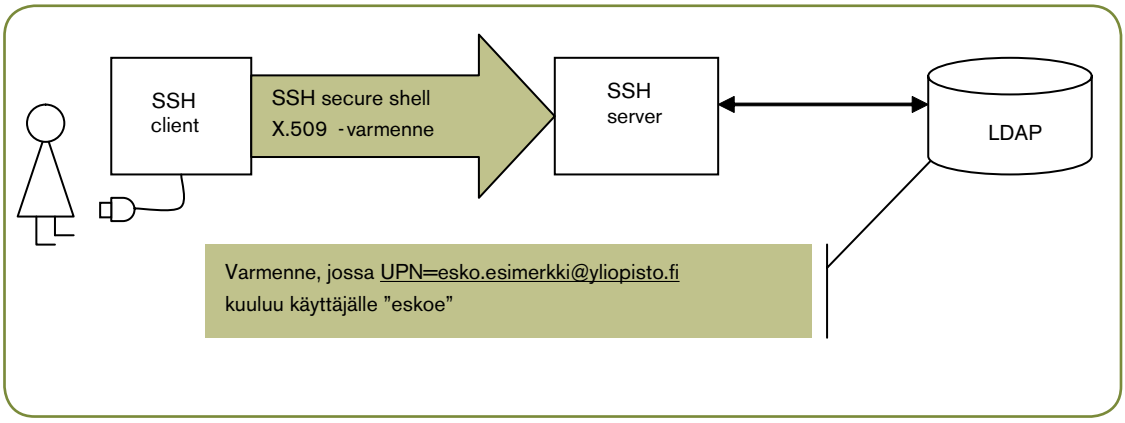
Kuvio 10. WWW-ympäristössä varmennekirjautuminen suositellaan suoritettavaksi SAML-tekniikan avulla.

Koska useimmissa yliopistoista on käytössä SAML/Shibboleth Identity Provider, työryhmä suosittaa, että varmennekirjautuminen tuodaan WWW-ympäristöön konfiguroimalla Identity Provider tukemaan sitä. WWW-palvelut (SAML Service Provider) puolestaan konfiguroidaan tukeutumaan kirjautumisessa Identity Provider -palvelimeen.

Tällöin riittää, että konfigurointi tehdään yhdessä paikassa, jonka jälkeen sen tuominen muihin WWW-palveluihin on helppoa. Samalla myös Haka-luottamusverkostoon saadaan käyttöön vahva autentikointi. Helsingin yliopiston tietotekniikkaosastolla oli vuonna 2006 pilotti vahvan autentikoinnin käytöstä Shibboleth-tekniikassa[8]. SAML 2.0 ja sen toteutus Shibboleth 2.x sisältävät aikaisempaa paremman tuen erivahvuisille autentikointimenetelmille.

7.3.5 SSH Secure Shell

SSH Communicationsin Tectia-tuoteperhe, joka sisältää SSH Secure Shell -asiakasohjelmiston ja palvelimen, tukee varmenneautentikointia. Asiakasohjelmisto asioi toimikortin kanssa PKCS#11-rajapinnan kautta. Myös OpenSSH-asiakasohjelmistoon on saatavissa PKCS#11-tuki[9].

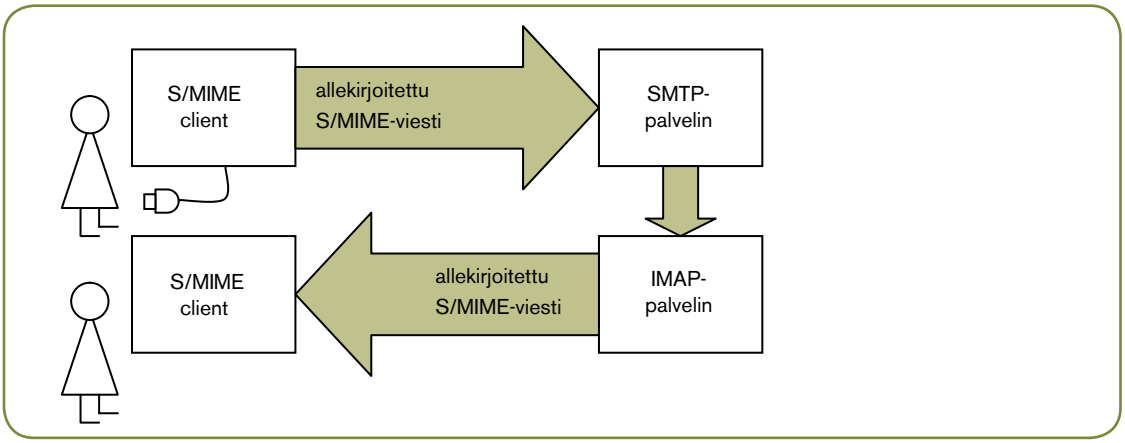


Kuvio 11. Varmennekirjautuminen SSH Secure Shell -yhteyksissä

8 http://www.helsinki.fi/~aulaskar/tietos/vetuma/doc/vetuma1.0/
9 http://alon.barlev.googlepages.com/openssh-pkcs11

7.3.6 Turvaposti

S/MIME-tekniikka mahdollistaa salatun ja/tai allekirjoitetun sähköpostin lähettämisen. S/MIME-tuki on saatavissa Microsoft Outlookiin CSP-rajapinnan kautta. Mozilla-pohjaiset sähköpostiasiakasohjelmistot osaavat hyödyntää PKCS#11-rajapintaa.



Kuvio 12. Sähköpostin allekirjoitus varmennekortin avulla

7.4 Kortin muut toiminnot

Edelliset kappaleet kuvasivat varmennekortilla olevan varmenteen käyttöä. Tässä alaluvussa käsitellään lyhyesti muita toiminnallisuuksia, jotka varmennekortille voidaan sijoittaa. Tässä esitetyille muille toiminnallisuuksille on leimallista, että ne eivät käytä lainkaan varmennekortin kontaktillista sirua, jolle varmenteet on sijoitettu. Sen sijaan varmenteen kanssa samaan muovialustaan on yhdistetty toiminnallisuuksia, jotka toimivat varmenteesta riippumatta.

Varmennekorttia voidaan käyttää yliopiston kiinteistön kulunhallinnassa. Tällöin käytetään tyypillisesti kontaktitonta RFID-tekniikkaa, ja kiinteistössä liikkuvalle henkilölle annettava RFID-tunniste (”RFID-tägi”) sijoitetaan samalle muoville, johon varmennekortti on sijoitettu. Periaatteessa myös varmennekortin kontaktillista sirua voitaisiin käyttää kulunhallinnassa, mutta kontaktittoman RFID-tunnisteen etuna on parempi luotettavuus ja kestävyys mm. erilaisissa sääolosuhteissa sekä suurempi nopeus myös vauhdikkaissa käyttötilanteissa.

Kulunhallinnan yhdistäminen varmennekorttiin käy tyypillisesti niin, että kulunhallintajärjestelmän toimittaja toimittaa kulunhallintaan tarkoitettuja, RFID-tunnisteen sisältäviä kulunhallintakortteja Väestörekisterikeskukselle, jonka alihankkija (PA Segenmark) poraa niihin reiän ja sovittaa reikään sirun varmenteita varten. Etukäteen tulee varmistaa, onnistuuko sirun upottaminen yliopiston käyttämään kulunhallintakorttiin. Käytännössä tämä vaatii kokeilemista.

Varmennekorttia voi myös käyttää visuaalisena tunnisteena eli henkilökorttina, jota virkamies pitää esillä. Väestörekisterikeskuksen tuotevalikoimaan kuuluvan ns. vakiotoimikortin pintaan painetaan pelkästään kortinhaltijan nimi, organisaatio sekä kortin sarjanumero ja voimassaoloaika sekä ohje hukkuneen kortin palauttamiseksi. Lisähinnasta varmennekorttiin voidaan yksilöidä myös organisaation oma visuaalinen ilme sekä kortin-

haltijan valokuva. Jos varmennekortti sisältää myös kulunhallinnan, kuten edellisessä kappaleessa on kuvattu, tulee etukäteen varmistaa, että kulunhallintakortin muoville on ylipäätään mahdollista tulostaa korttitulostimella.

Varmennekorttiin voidaan myös yhdistää maksamisen liittyviä toimintoja, esimerkiksi Suomen Lyyra Oy:n Lyyra-kortti, jota voidaan käyttää esimerkiksi henkilökuntalounaan maksamiseen. Yhdistäminen tapahtuu upottamalla Lyyra-korttiin varmenteet sisältävä siru.

8 Liittymät muuhun toimintaan

Tässä luvussa tunnistetaan varmennekortin liittymät hallinnonalan muuhun toimintaan ja rinnakkaisiin hankkeisiin tai palveluihin.

8.1 Opetusministeriön hallinnonalan tietohallintostrategia

Opetusministeriö on marraskuussa 2006 antanut hallinnonalaa koskevan tietohallintostrategian vuosille 2006-2015. Tietohallintostrategian strategisen linjauksen 4 mukaan *opetusministeriön hallinnonalalla käytetään tarkoituksenmukaisella tavalla markkinoilta saatavia ja valtionhallinnon yhteisiä IT-palveluja, muun muassa (…) VRK:n varmennepalveluja organisaatioille ja kansalaisille. Linjauksen avaintoimenpiteeksi on kirjattu, että virkakorttien käyttämiseen ja hallinnointiin määritellään yhtenäiset periaatteet ja sähköinen allekirjoitus otetaan käyttöön hallinnonalan sisäisessä virallisessa asiakirjaliikenteessä.*

8.2 HSTYA-projekti 2000-2002

HSTYA (henkilön sähköinen tunnistaminen yliopistoissa ja ammattikorkeakouluissa) oli korkeakoulujen, opiskelijajärjestöjen ja tieteen tietotekniikan keskus CSC:n yhteishanke, jonka päämääränä oli toimikorttien ja varmenteiden käyttöönottaminen korkeakouluissa opiskelijoille ja henkilökunnalle. Hankkeen laajuus oli 16 henkilövuotta, josta puolet käytettiin korkeakouluissa järjestetyissä yhdeksässä pilotissa. Hanke näki varmenteellisten toimikorttien käyttöönoton mahdolliseksi ja esitti loppuraportissaan[10] seitsemän johtopäätöstä ja niihin liittyvää toimenpide-ehdotusta. Johtopäätökset ovat

1. Julkisen avaimen järjestelmän perusta on toimiva, ja sen varaan voidaan rakentaa tulevaisuudessa myös korkeakoulujen järjestelmissä käyttäjän tunnistaminen, vaikka julkisen avaimen järjestelmää toteuttavissa toimikorttiratkaisuissa onkin vielä joitain puutteita.
2. Valvomattomien työasemien tarjoaminen asiointipäätteiksi sisältää tietoturvariskejä, joihin liittyvät vastuukysymykset ja varotoimet tulee selvittää ennen julkisen avaimen järjestelmän ottamista käyttöön korkeakoulujen opiskelijatyöasemissa.

---

10 http://www.csc.fi/csc/julkaisut/oppaat/pdfs/pdf-versiot/hstya.

3. Korkeakoulujen kannattaa edetä kehitystyössä vaiheittain: ensin rakennetaan keskitetty käyttäjähallinto, sitten mahdollistetaan toimikorttikirjautuminen käyttäjien kannalta keskeisiin palveluihin ja vasta näiden vaiheiden jälkeen järjestetään henkilövarmenteet kattavasti henkilöstön ja opiskelijoiden käyttöön.
4. Julkisen avaimen järjestelmän käyttöönotto korkeakoulussa edellyttää käytännön kokemusten hankkimista ja ylläpitohenkilökunnan kouluttautumista sekä käyttäjätuen järjestämistä. Tämän vuoksi järjestelmä kannattaa ensin tarjota erikseen määriteltyjen henkilöstöryhmien käyttöön.
5. Kunkin korkeakoulun kannattaa arvioida omalla kohdallaan julkisen avaimen järjestelmän eri toteutustavat kustannuksineen ja hyötyineen. Toimikortteihin perustuvan julkisen avaimen järjestelmän käyttöönotto koko korkeakouluyhteisössä ei vaadi yhtä yhteistä sähköistä korkeakoulukorttia.
6. Korkeakouluissa on ryhdyttävä määrätietoisesti kehittämään sähköisiä palveluita ja toimintaprosesseja, mikäli tietoturvatason kohoamisen lisäksi julkisen avaimen järjestelmästä haetaan palvelujen laadun kohoamista tai kustannussäästöjä.
7. Korkeakoulujen väliset organisaatiorajat ylittävä verkkopalveluiden käyttö edellyttää kansallisia ratkaisuja käytännöistä ja tekniikasta sekä käyttäjähallinnon tietojärjestelmien kehittämistyön kansallista koordinointia.

Hankkeessa ja hankkeen jälkeen tuotettiin PKI-toimikorttien käyttöönottoon liittyvää ohjeistusta ja jaettiin PKI-toimikortteja kaikkiin korkeakouluihin tekniikan testaamista varten. Vaikka hanke ei johtanutkaan PKI-toimikorttien laajamittaiseen käyttöönottoon, siinä tuotettiin runsaasti materiaalia, josta suuri osa on edelleen hyödyllistä.

HSTYA hankkeeseen osallistunut Olavi Manninen Kuopion yliopistosta kirjoittaa kommenteissaan:

Koska olin aikanaan mukana HSTYA-projektin ohjausryhmässä, haluan vielä listata ne asiat, joihin korttien käyttöön tuolloin mielestäni kaatui:

- Kortin kuviteltiin ratkaisevan kaikki käyttäjien tunnistukseen ja käyttövaltuuksiin liittyvät ongelmat. Pelkkä kortti ei riitä, käyttäjähallinta, roolit, hakemistot ja prosessit on oltava kunnossa ennen korttien käyttöönottoa.

- Henkilökohtainen kortti ei sovellu kovin hyvin yritys/virastokortiksi.

- Suurimpia tarpeita vahvaan tunnistautumiseen ja varmennekorttien käyttöön olisi ollut tietyissä hallinnollisissa sovelluksissa, mutta (juuri) missään niistä ei ollut valmiina tukea varmennekorttien käytölle.

- Tekniikka ei ollut muutenkaan riittävän kypsää/yhteentoimivaa HSTYA-projektin aikaan, mm. ei tainnut löytyä yhtään sähköpostiohjelmaa, jonka kanssa korttia olisi voinut käyttää sekä sähköpostin allekirjoitukseen ja salaukseen. Ilmeisesti tilanne on parantunut näiden vuosien aikana.

Ja: varmennekorttien käyttöön tarvittava tekniikka oli KALLISTA silloin ja vieläkin

8.3 Haka-luottamusverkosto

HSTYA-projektin toimenpide-ehdotuksen mukaisesti korkeakoulut ja tieteen tietotekniikan keskus CSC käynnistivät HAKA-projektin, joka johti Haka-luottamusverkoston[11] syntyyn elokuussa 2005. Haka-luottamusverkosto laajentaa korkeakoulujen paikalliset käyttäjätunnistusjärjestelmät ylettymään myös korkeakoulujen ulkopuolelle: loppukäyttäjä korkeakoulussa voi käyttää kotikorkeakoulunsa käyttäjätunnusta (identiteettiä) myös korkeakoulunsa ulkopuolella oleviin (WWW-pohjaisiin) palveluihin kirjautumiseen. Tällä hetkellä Hakassa on mukana 16/20 yliopistoa[12], ja se kattaa 96% loppukäyttäjistä yliopistoissa. Hakan tekninen toteutus perustuu SAML/Shibboleth-tekniikkaan.

Tällä hetkellä Hakaan liittyneille korkeakouluille asetettu minimivaatimus käyttäjän henkilöllisyyden todentamiselle on salasana, jolta edellytetään vähintään 8 merkin pituutta. SAML-tekniikka, erityisesti sen versio 2.0, tukevat myös laajempaa henkilöllisyyden todentamisen menetelmien valikoimaa: erityisen sensitiivinen palvelu voi esimerkiksi pyytää PKI-toimikortilla tapahtuvaa henkilöllisyyden todentamista. Helsingin yliopiston tietotekniikkaosasto on pilotoinut PKI-toimikortilla ja VETUMA-palvelun kautta tapahtuvaa vahvaa henkilöllisyyden todentamista Shibboleth-tekniikan yhteydessä vuonna 2006. Tähän mennessä salasanaan perustuva henkilöllisyyden todentaminen on kuitenkin riittänyt kaikille Hakaan rekisteröidyille palveluille.

Haka-luottamusverkosto on siirtymässä SAML 2.0 -tekniikan käyttöön. Siirtymäaika on alkanut vuonna 2008 ja vuoden 2010 lopussa viimeisenkin palvelimen on määrä tukea SAML2:a. Opetusministeriön hallinnonalan tietohallintostrategiaan on kirjattu kehittynyt sähköinen allekirjoituksen toteuttaminen Haka-palvelujen yhteyteen.

Haka ei edellytä virkavarmenteiden käyttöä, mutta tarjoaa mahdollisuuden hyödyntää virkavarmenteita WWW-pohjaisten palveluiden kirjautumisessa perustasoa sensitiivisemmissä palveluissa standardin SAML 2.0 -tekniikan kautta. Työryhmä suosittelee, että SAML-tekniikkaa hyödynnetään varmennekirjautumisessa WWW-ympäristössä myös yliopiston sisällä.

Varmennekortin avulla käytettäviltä palveluilta tulisikin edellyttää Haka-luottamusverkoston järjestelmävaatimusten mukaisuutta.

Järjestelmien sekä palveluiden toimittajien on syytä huomioida vaatimus Haka-yhteensopivuudesta.

8.4 ValtIT:n Virtu-kärkihanke

Valtiovarainministeriön ValtIT-hankkeeseen sisältyvä Virkamiehen tunnistaminen ja käyttöoikeuksien hallinta -kärkihanke (Virtu) tähtää yhteensopivien tietojärjestelmien rakentamiseen virkamiehen virastorajat ylittävässä tunnistamisessa. Hankkeen esitutkimusvaihe 11/2006-5/2007 jätti esitutkimusraportin[13], joka suosittelee Virkamiehen tunnistamisen ja käyttöoikeuksien hallinnan toteuttamista SAML 2.0 -tekniikan avulla rakennettavan Virtu-luottamusverkoston varaan.

---

11 **http://www.csc.fi/haka**
12 **http://www.csc.fi/hallinto/haka/luottamusverkosto/jasenet**
13 **http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070625Virkam/name.jsp**

Hankkeen toteutusvaihe on alkanut 10/2007 ja päättyy vuonna 2009 lopussa, jolloin Virtu-luottamusverkosto on otettu käyttöön. Toteutusvaiheen toimeksianto[14] lähtee siitä, että Virtu-luottamusverkostosta tulee julkishallinnon yhteinen palvelu, joka sulkee sisäänsä myös välillisen valtiohallinnon, kuten valtion budjettitaloudesta irrotetut yliopistot.

Virtu-luottamusverkosto tukeutuu Tietoturvatasot-kärkihankkeeseen käyttäjähallinnon tietoturvatason asettamisessa. Hankkeen esitutkimusraportissa on otettu lähtökohdaksi, että Virtu-hanke ei edellytä virkavarmenteita, mutta luo sille edellytyksiä tarjoamalla joustavan siirtymäpolun kohti virkavarmenteiden käyttöä. Hankkeen esitutkimusraportissa ei oteta kantaa siihen, onko virkavarmenne varmennekortilla vai muulla alustalla.

8.5 ValtIT:n Tietoturvatasot-kärkihanke

Tietoturvatasot ovat luokiteltuja turvatoimenpide- ja menettelyvaatimuksia, jotka kohdistuvat turvattavan kohteen suojaamiseen. Turvatasot ovat yhteensopivia kansainvälisten standardien, laatumallien ja hyvien käytäntöjen kanssa. Valtionhallinnossa yhteiselle (perus)turvatasolle on mahdollista asettaa yhtenäiset vaatimukset, kun turvattavista kohteista on sovittu ja turvatavoitteet päätetty.

Tietoturvatasot-hanke on käyttänyt kuutiomalleja (kuva) suojattavien kohteiden tietoturvatason visualisoimiseen. Kukin taso (toistettava, määritelty, hallittu, optimoitu) muodostaa oman viipaleensa kuutiossa, ja asettaa edellistä tasoa korkeammat vaatimukset suojattavan kohteen turvaamiselle. Toisaalta kohteen turvaaminen sisältää tietoturvallisuuden eri osa-alueisiin (henkilöstö, tietoaineistot, tilat jne.) sisältyviä toimenpiteitä, joista osa on luonteeltaan toimenpiteisiin ja tekniikkaan liittyviä (kuution alin taso), osa toimintaan ja prosesseihin liittyviä (kuution keskitaso) ja osa strategiseen johtamiseen liittyviä (kuutio ylätaso). Lisäksi organisaation on oltava riittävän kypsä ja kyvykäs hallitsemaan tietoturvallisuutta.

Tietoturvatasot-kärkihankkeen esitutkimusvaihe jätti esitutkimusraporttinsa[15] kesäkuussa 2007. Hankkeen toteutusvaiheessa laadittava Tietojärjestelmien hallinnan kypsyyskriteerit -ohje ottaa kantaa myös vahvan tunnistuksen käyttöön.

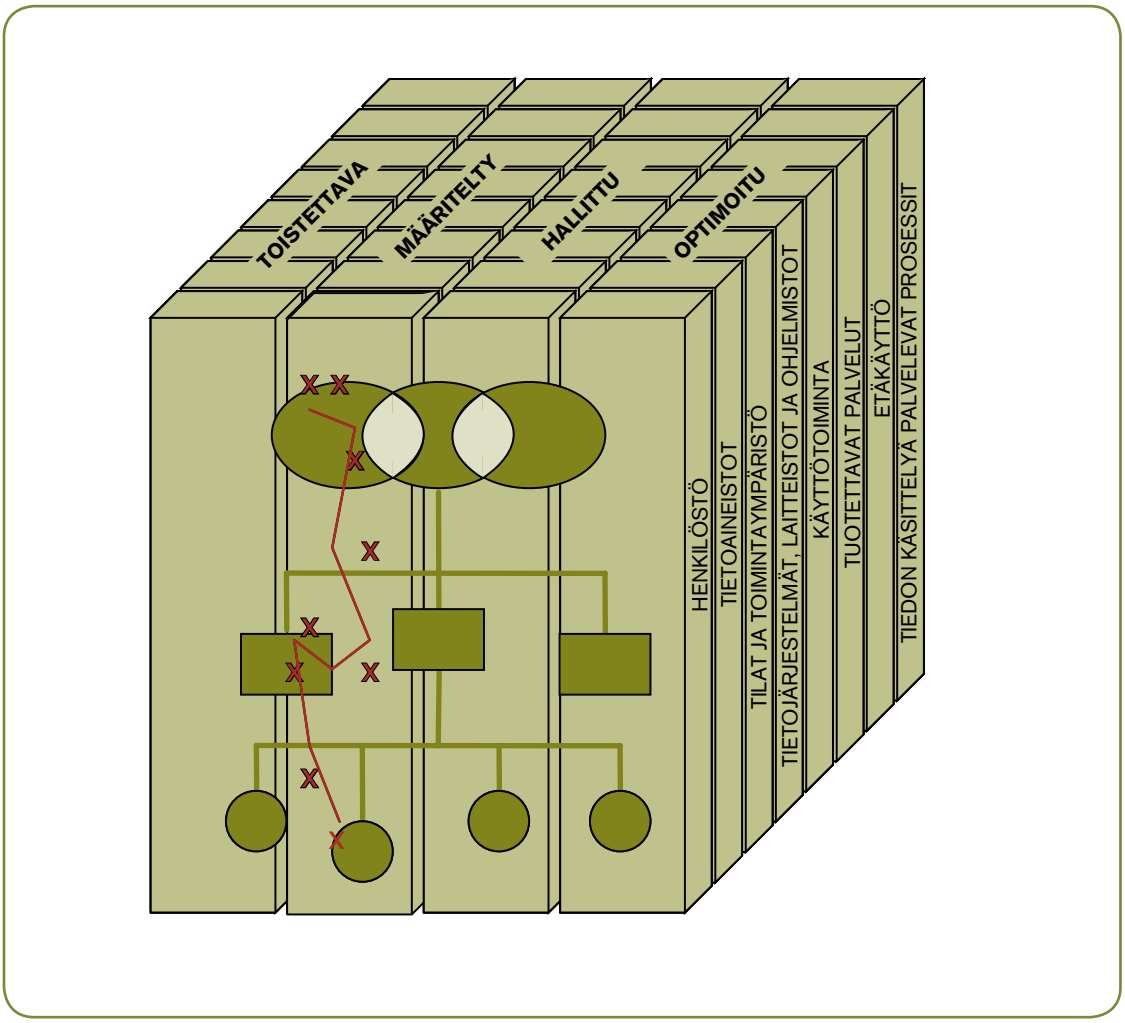
8.6 Puitesopimus virkakorteista

Hankintalain mukaan ministeriöt eivät voi solmia puitesopimuksia hallinnonalan virastoille, vaan puitesopimusten solmiminen on sälytetty yhteishankintayksikölle, joka on Hansel Oy. Valtiontalouden tarkastusvirasto (161/2008, s. 80) on nostanut esiin tarpeen tehdä virkakortteja koskeva kilpailutus, jonka Hansel toteuttaisi.

---

14 Virkamiehen tunnistamisen ja käyttöoikeuksien hallinnan luottamusverkosto, toteutussuunnitelma (luonnos 12.10.2007)

15 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070626Valtio/name.jsp



Kuvio 13. Tietoturvatasot

9 Johtopäätökset sekä jatkotoimenpiteet

Projekti on selvittänyt laatuvarmenteen sisältävän varmennekorttien, ns. virkakortin, käyttöönottoa yliopistoissa. Jos varmennekortit päätetään ottaa yliopistoissa käyttöön, projekti on koostanut joukon suosituksia, joita suositellaan noudatettavaksi käyttöönoton yhteydessä.

Tehtyjen selvitysten ja saatujen kommenttien perusteella projektiryhmä katsoo, että ennen varmennekorttien mahdollista laajamittaista käyttöönottoa tulee eri todentamismenetelmien käyttöä yliopistoissa vertailla tarkemmin palvelukohtaisesti ja tarvepohjaisesti pilottien avulla. Projektin aikana on käynyt ilmi useita käyttöönoton toteuttamiseen liittyviä tekijöitä sekä toimintaympäristössä tapahtuneita muutoksia, joiden perusteella yhteisesti toteutettu jatkoselvittely voi olla hyödyllisempää kuin nopeasti toteutettava laajamittainen yhteinen käyttöönotto. Ei kuitenkaan ole esteitä toteuttaa varmennekorttien käyttöönottoa paikallisesti jo nyt.

Eri toimittajien varmennekorttien lisäksi tulisi tarkemmin vertailla muitakin todentamisratkaisuja, kuten mobiilivarmenteita, muita vahvan todentamisen tekniikoita, todentamista pankkipalvelun kautta sekä myös salasanoihin perustuvia ratkaisuja.

Lisäksi valitut ratkaisut tulee tarvittaessa kilpailuttaa uudelleen ennen laajamittaisia hankintoja.

Tällä hetkellä tarjolla oleva palvelutaso laatuvarmenteiden osalta ei ole riittävän nopea ja joustava soveltuakseen laajamittaisesti yliopistojen tarpeisiin. Logistiikan kehittämisen tavoitteena tulisi olla, että varmenteen voi saada esimerkiksi palvelupisteessä odottaessa, samoin kuin uuden salasanankin. Erityisesti logistiikassa tulisi huomioida, että osa henkilökunnasta saattaa työskennellä etätyöpisteissä tai ulkomailla.

Vahvan todentamisen piiriin kuuluvien palvelujen määrittely on syytä käynnistää palveluista, joissa Valtiokonttori edellyttää sitä.

Jatkossa palveluita on syytä tuoda vahvan todentamisen piiriin tietoturvavaatimusten ja soveltuvuuden testaamisen jälkeen. Sama pätee myös mahdollisten uusien palveluiden, kuten Lyyra-korttiin liitettyjen palveluiden, liittämiseen todentamisratkaisuun.

Käyttöönoton toisessa vaiheessa tulisi harkita etäkäytön ja etäylläpidon siirtämisestä vahvan todentamisen taakse. Osan etäylläpidosta voinee periaatteessa toteuttaa VRK: n laatuvarmenteella, muilta osin voinee käyttää myös muita vahvan todentamisen menetelmiä, esimerkiksi mobiilivarmennetta.

Seuraavassa mahdollisessa käyttöönottovaiheessa voidaan ottaa käyttöön jo palveluita, joissa käyttäjien lukumäärä on hyvin laaja, kuten henkilökunnan työasemakirjautuminen. Erityisesti sellaisissa projekteissa tulee tekniikan toimivuus, käyttömukavuus, kustannukset ja turvallisuuden toteutus selvittää tarkasti ennen käyttöönottopäätöksen tekoa.

Uusien todentamisratkaisujen käyttöönoton aikataulu riippuu paljolti siitä, miten ja millä teknologialla yliopistojen sähköiset palvelut kehittyvät. Todentamisratkaisut seuraavat tätä kehitystä. Aikatauluun vaikuttaa myös lainsäädännön ja muiden vaatimuksien kehittyminen yliopistojen toimintaympäristössä.

Kustannuksissa tulee huomioida paitsi kortteihin liittyvät välittömät kustannukset myös epäsuorat järjestelmäintegrointiin ja hallinnollisiin toimenpiteisiin liittyvät kustannukset. Kustannuksiin tulee suhteuttaa käyttöönotosta saavutettava taloudellinen hyöty.

9.1 Käyttöönoton edellytykset

Ennen kuin käyttöönottoa ryhdytään toteuttamaan laajemmin, tulee seuraavat tekniset sekä hallinnolliset toiminnallisuudet todentaa pilottihankkeen avulla:

- Uuden korttitoimittajan PA Segenmarkin toimittamien korttien ja Fujitsu Digisign -ohjelmiston tekninen toimivuus nykyisten kortinlukijoiden ja käyttöjärjestelmien kanssa tulee varmistaa.
- Korttien kustannukset tulee määritellä yliopistojen käytettävissä olevalla kilpailutetulla hankintasopimuksella.
- Korttien tilaamiseen liittyvä logistiikka aika-rajoineen tulee määritellä ja sopia yhteisesti.
- Tulee laatia yhteinen ohje sekä loppukäyttäjille että ylläpitäjille siitä, miten todentaminen varmennekorttien kanssa toteutetaan turvallisesti ja tehokkaasti.

9.2 Käyttöönotto

Projektiryhmä katsoo, että tietoturvavaatimusten mukainen sähköinen asiointi tulisi valmisteilla olevan tietoturva-asetuksen mukaisten tärkeysluokiteltujen toimintojen osalta pääasiallisesti perustua vahvaan käyttäjän todentamiseen.

Ensisijaisesti vahvan todentamisen vaatimus tulee perustua tiedon ja palveluiden yliopistokohtaiseen luokitteluun.

Todentamismenetelmää valittaessa on syytä pitää mielessä, että todentamistekniikka on vain yksi turvallisuustekijä monen muun joukossa.

Varmennekorttien, kuten myös muiden todentamistekniikkojen, käyttöönotolla on kustannuksensa ja haittansa. Käyttöönoton hyödyt voivat ilmetä ennen kaikkea turvallisuuden parantumisena, mutta tietyissä tapauksissa myös käyttömukavuuden parantumisena, koska salasanojen jatkuva vaihtaminen vähenee.

Todentamisratkaisujen käyttöönotto tulee aina suunnitella sekä pilotoida huolellisesti palvelukohtaisesti, jotta tärkeiden palveluiden käytettävyys ei käyttöönoton vuoksi heikkene.

Työryhmän minimisuositus on, että jokaisella yliopistolla on laatuvarmenne kaikkien niiden henkilöiden käytössä, joilla se työtehtävien vaatimusten mukaan tulee olla. Lisäksi henkilökunnalla on kuvallinen henkilökortti, johon yliopiston omien tarpeiden mukaan lisätään muita lisäpalveluita. Tämä minimikorttiratkaisu tulisi olla kaikkien yliopistojen

käytössä vuoden 2009 syksyllä, perustuen tietoturvallisuuden minimivaatimuksiin sekä hyvään hallintotapaan.

Tuleville kehitys- ja laajentumispoluille on monta mahdollisuutta. Yksi mahdollisuus on, että yliopistot ottavat käyttöön ns. monipalvelukortin, toinen kehitystie on muiden vahvan todentamisen menetelmien käyttöönotto. Toisaalta tulee myös eräänä realistisena skenaariona huomioida nykyistenkaltaiset salasanapohjaiset todentamisratkaisut.

Eräänä vaihtoehtona on, että jatkossa kuitenkin lisäselvitysten jälkeen päädytään suosittelemaan yliopistoyhteisölle henkilökortin ja laatuvarmenteen sisältävää yhdistelmäkorttia. Monipalvelukortti sisältää kaikki tärkeimmät teknologiat: Kontakti-siru, RFID-tunniste, kuva ja tarvittavat viivakoodi- ym. painatukset. Kortille voi lisätä ja poistaa henkilölle myönnettyjä palveluita työnantajan tarpeen mukaan. Yliopisto päättää itse, mitä palveluita se haluaa ottaa käyttöön, samoin kenelle henkilölle varmennekortteja annetaan. Tämä malli perustuu Väestörekisterikeskuksen ratkaisumalliin sekä Väestörekisterikeskuksen ja Suomen Lyyra Oy:n antamiin tietoihin.

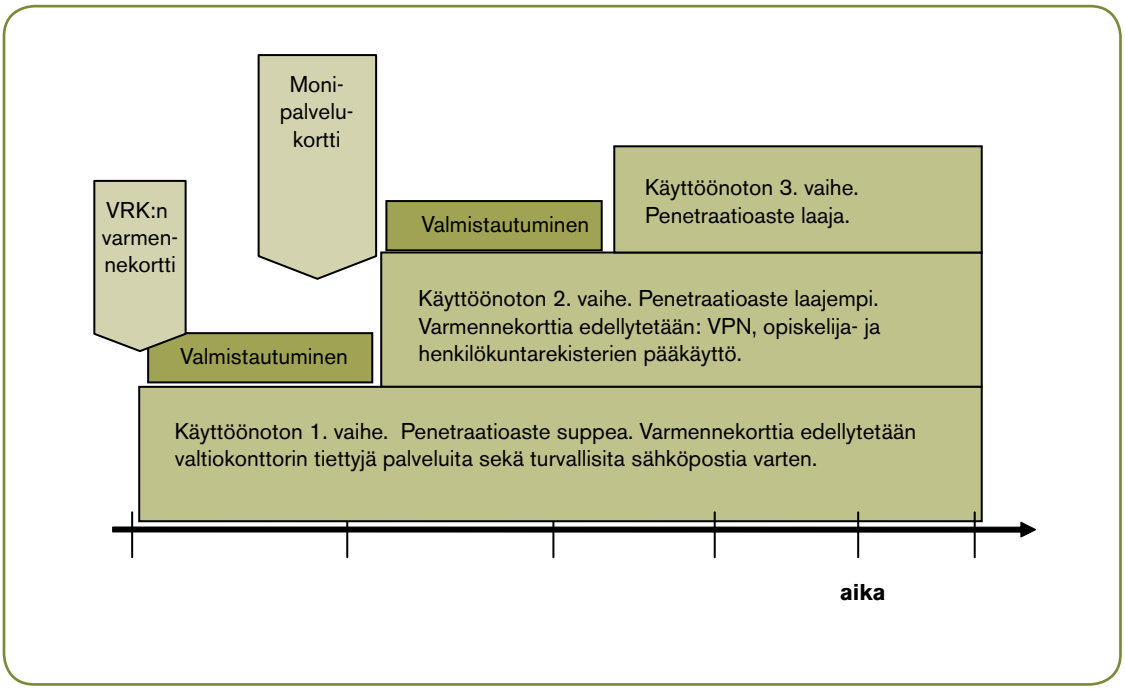
Perusteluina ovat

- Laatuvarmenne luo edellytykset yhtenäisten turvallisuutta vaativien tunnistamis- ja todentamispalveluiden pitkäjänteiseen kehittämiseen yliopistojen tietojärjestelmissä.
- Yhdistelmäkortti tukee yliopistoyhteisöjen nykyistä kehitystyötä ja korttiratkaisuja ilman kalliita infrastruktuurimuutoksia.
- Ratkaisu tukee myös nykyisten palvelutoimittajien edellytyksiä luoda yhä parempia palveluita.
- Yliopistoyhteisöjen yhteinen korttiteknologiaratkaisu mahdollistaa tulevaisuudessa pitkäjänteisen kehittämisen myös yliopistojen yhteistyönä.
- Ratkaisu täydentää Haka-luottamusverkoston palveluita tuomalla siihen myös henkilön vahvan tunnistamisen.
- Monipalvelukortti mahdollistaa ja tukee identiteetin hallinnan johtamisen ja kehittämisen uudistamista yliopistoissa.
- Monipalvelukortin hyödyt suhteessa kustannuksiin vaikuttavat olevan muita korttivaihtoehtoja edullisempia, kun huomioidaan prosesseissa saatavat työaikasäästöt.
- Monipalvelukortti luo yleensä parhaan edellytyksen henkilön identiteetin tunnistamiseen sekä turvalliseen todentamiseen eri tilanteissa.
- Ratkaisu mahdollistaa asteittaisen siirtymisen nykyisistä toimintamalleista tavoitetilaan.

Toimittajat ovat luvanneet, että tämä uusi ratkaisu on käytettävissä vuoden 2009 aikana. Yliopistojen siirtyminen uuteen monipalvelukorttiin ajoittuu useammalle vuodelle. Kukin yliopisto päättää itse suosituksen soveltamisesta ja siirtymäaikataulusta.

Tämä malli perustuu monipuoliseen teknologiaan ja se luo hyvät edellytykset lisätä henkilökunnan luotettavaa todentamista sekä nykyisissä että tulevissa tarpeissa. Se luo monipuolisen ja yhtenäisen infrastruktuurin yliopistoyhteisöjen henkilöiden tunnistamiseen. Monipuolinen tekninen alusta ei yksin riitä, vaan se edellyttää yhteisten palveluiden jatkuvaa kehittämistä tunnistuksen piiriin. Tätä ratkaisua voi verrata Haka-luottamusverkostoon ja siihen kehitettäviin palveluihin.

Ennen päätöksentekoa tulee myös verrata varmennekorttipohjaista ratkaisuja muihin todentamismalleihin, kuten mobiilivarmenteiden tai pankkipalvelun käyttöön sekä myös salasanoihin perustuviin ratkaisuihin.



Kuvio 14. Mahdollinen vaihtoehtoinen kehityspolku varmennekorttien käyttöönotolle

Nykyisen laatuvarmenteen suuria haittapuolia on palvelun hitaus ja jäykkyys dynaamisessa yliopistoympäristössä. Tavoitteena tulisi olla, että käyttäjä voi tarvittaessa saada uuden varmenteen odottaessa, aivan kuten salasanankin.

9.3 Ympäristössä tapahtuneiden muutosten huomioiminen

Projektiryhmä on todennut päätöskokouksessaan 6.6.2008, että projektin aikana ja kommenttikerroksen jälkeen on tapahtunut merkittäviä muutoksia toimintaympäristössä:

- Uuden yliopistolain valmistelu
- Valtiontalouden tarkastusviraston raportin (Tunnistuspalveluiden kehittäminen ja käyttö julkisessa hallinnossa.) julkaisu, jossa mm. esitetään kysymyksiä Väestörekisterikeskuksen roolista
- Korttiohjelmistojen uudet versiot, joita ei vielä ole testattu kattavasti
- Lyyran hybridi-kortti, jossa kontaktisirun lisäksi RFID-siru
- Mobiilivarmenteisiin liittyvä selvitystyö.

Todettiin, että ympäristössä tapahtuneet muutokset ovat olleet merkittäviä ja niistä johtuen projektiryhmä täsmensi suosituksia jatkotoimenpiteistä.

Todettiin että projektiryhmä on toimeksiantonsa mukaisesti määritellyt yhteisiä suosituksia VRK:n varmennekorttien käyttöönotosta, elinkaaren hallinnasta ja ylläpidosta yliopistoissa. Projektiryhmän suosituksia voi ryhtyä toteuttamaan.

Saadun palautteen ja ympäristössä tapahtuvien muutosten perusteella projektiryhmä suosittelee ennen laatuvarmennepohjaisten korttien (ns. VRK:n virkakorttien) mahdollista laajamittaisempaa käyttöönottoa, että eri todentamismenetelmien, kuten mm. mobiili-

varmenteiden tai kolmannen osapuolten tai omavarmenteiden käyttöä yliopistoissa tulee vertailla tarkemmin tuotannollisten pilottiprojektien avulla.

9.4 Ehdotus jatkotoimenpiteiksi

- Koska teknologia, ratkaisut ja kustannusvaikutukset muuttuvat nopeasti, tulee ennen uusien todentamisratkaisujen käyttöönottoprojektia tarkistaa todentamisratkaisujen ajankohtainen tilanne.
- Jotta yliopistot saisivat parempaa tietoa päätöksenteon pohjaksi, tulisi ennen käyttöönottoprojekteja toteuttaa useamman vuoden ohjelmaan perustuen koordinoituja palvelukohtaisia pilottiprojekteja, jotka tuottavat konkreetista tietoa tekniikasta, käyttöönotosta ja käytetyistä prosesseista.
- Tulisi luoda yksityiskohtaisempia palvelupohjaisia teknisiä että hallinnollisia käyttöönottomalleja.
- Mobiilivarmenteiden käytön tekniikkaa ja hallinnointia yliopistoissa on syytä myös seurata aktiivisesti yhteistyössä Helsingin yliopistossa käynnistyneen projektin kanssa.
- Yhteistyötä ja rajapintoja Lyyra-kortin kanssa on syytä seurata ja kehittää myös projektin päättymisen jälkeen myös tietoturvanäkökulmat huomioiden.
- Olisi syytä myös harkita, voisiko olemassa olevia todentamismenetelmiä kehittää esimerkiksi salasanan laadun tarkistamisen menetelmillä.
- Uusia ratkaisuja on syytä etsiä tiiviissä yhteistyössä Haka-luottamusverkoston kanssa.
- Projekti ehdottaa, että yliopistojen yhteinen tietoturvaryhmä, Sec-ryhmä, saa tehtäväkseen seurata aktiivisesti varmennekortteihin perustuvan todentamistekniikan käyttöönottoon liittyvä mahdollisuuksia yliopistoissa sekä tehdä asiasta vuosittain toimenpide-ehdotuksia.
- Projekti ehdottaa, että opetusministeriön ja hallinnonalan tietohallinnon johtoryhmä (OpIT) voi tehdä päätöksiä käyttöönottoprojektien edistämisestä ja viedä esityksiä eteenpäin yliopistojen tietohallintojohtajien sekä IT-pääsihteerin käsiteltäväksi.
- Projekti ehdottaa kolmevuotisen kehitys- ja pilotointiprojektin käynnistämistä varmennekorttien käyttöönotosta yhteistyössä yliopistojen tietohallintojohtajien ja tietoturvapäälliköiden sekä vastaavista hankkeista paljon kokemusta omaavan Haka-luottamusverkoston kanssa.
- Kehitys- ja pilotointiprojektia varten haetaan erikseen sovittavan yliopiston toimesta hankerahoitusta OPM:ltä. Yliopistojen IT-pääsihteeri sekä tämän projektin sihteeri valmistelevat hakemusta.

10 Projektin tuloksien hyödyntäminen

Projektiryhmä luovuttaa tämän loppuraportin projektin toimeksiantajalle sekä mahdollisesti julkaistavaksi OPM:n tai CSC:n julkaisusarjoihin.

Tarve ottaa käyttöön entistä tukevampia mutta joustavia todentamismenetelmiä tulee jatkossa kasvamaan.

Projekti esittää vertailevan kehitys- ja pilotointiprojektin käynnistämistä vahvan todentamisen menetelmien käyttöönotosta yliopistoissa. Projekti ehdottaa, että yliopistojen IT-pääsihteeri sekä projektisihteeri laativat projektitoimeksiannon sekä valmistelevat hakemusta rahoitusta varten yhteistyössä IT-johtajien työvaliokunnan kanssa. Tämä edellyttää sitä, että yliopistot päättävät tukea yhteisiä pilottihankkeita.

Todentamisratkaisujen kustannukset tulisi mieluiten määritellä siten, että yliopistot voisivat hyödyntää niitä valmiiksi kilpailutetulla hankintasopimuksella.

Projektin tavoitteet voidaan saavuttaa ja tulokset voidaan hyödyntää parhaiten etenemällä esitetyllä tavalla käyttöönotossa järjestelmällisesti yhteisten pilottiprojektien kautta ja raportoimalla kokemuksista yhteistä osaamista kartuttaen.

Projektin tuloksia voi varmennekorttien sekä myös muiden todentamisratkaisujen käyttöönottoon liittyen hyödyntää parhaiten aktiivisella yhteistyöllä ja viestinnällä myös projektin päättymisen jälkeen niin yliopistojen välillä kuin myös yliopistojen ja muun valtiohallinnon kesken. Myös kansainvälisellä tasolla on hyvä harjoittaa yhteistyötä sekä verrata kokemuksia ja vaihtaa tietoja tässäkin asiassa.

11 Liite A: Varmennekortteihin liittyviä käsitteitä

Toimikortti, älykortti, suoritinkortti, sirukortti (smart card)	**Toimikortti** (synonyymejä: älykortti, sirukortti, suoritinkortti) on tyypillisesti luottokortin tai matkapuhelimen liittymäkortin kokoinen laite, joka sisältää sirun. **Kontaktillisen toimikortin** tunnistaa siinä olevista kontaktipinnoista, joiden kautta kortinlukija asioi kortin kanssa. **Kontaktittomassa toimikortissa** kommunikointi tapahtuu RFID-tekniikalla, ja RFID-tunniste on kokonaan piilossa kortin muovin sisällä. Toimikortilla on kolme perustavanlaatuista ominaisuutta 1) suoritin ja sisäistä laskentakapasiteettia (erona mm. kameroiden muistikorttiin) 2) pieni koko (kulkee mukana) 3) peukalointia sietävä rakenne (korkea tietoturvallisuus) Toimikortteja käytetään erityisesti korkeaa turvallisuutta vaativiin tarkoituksiin: sirullisia pankkikortteja maksamiseen, matkapuhelimen liittymäkorttia puhelinliittymän todentamiseen, matkakorttia maksamiseen joukkoliikenteessä ja kulkukorttia kiinteistön pääsynhallinnassa. Tässä dokumentissa keskitytään varmennekorttiin, jota käytetään loppukäyttäjän todentamiseen avoimessa tietoverkossa. Samalle muoville voidaan kuitenkin integroida useita toimintoja, esimerkiksi kulunhallinta tai maksaminen henkilöstöravintolassa.
Toimikortinlukija (smart card reader)	Toimikortti tarvitsee aina **toimikortinlukijan**, joka voi olla esim. kortinlukija työasemassa, pankkiautomaatissa tai sähköisesti lukitussa ovessa. Myös matkapuhelimen sisällä on kortinlukija liittymäkorttia varten. Työasemaympäristössä kortinlukijat on usein integroitu työaseman tai näppäimistön kotelointiin tai ne voivat olla erillisiä, USB-väylään tai PC-korttipaikkaan liitettäviä lisälaitteita. Harhaanjohtavasta nimestään huolimatta kaikilla kortinlukijoilla voi myös kirjoittaa kortille, tai pyytää korttia tekemään muita operaatioita kuten salaamaan viestejä.
Varmenne (certificate)	**Varmenne** on merkkijono, jonka avulla henkilö (varmenteen haltija) voidaan tunnistaa tietoverkossa. Varmenteen avulla voidaan lähettää myös salattua sähköpostia tai todentaa dokumentin digitaalinen allekirjoitus. Varmenne voidaan antaa palvelimelle (palvelinvarmenne), mutta tässä dokumentissa ollaan kiinnostuneita vain henkilöillä (yliopiston virkamiehille) annettavista varmenteista (henkilövarmenne). Varmenne sisältää haltijansa nimen ja hänet yksilöivän tunnisteen. Lähtökohtaisesti varmenne talletetaan julkiseen varmennehakemistoon. Jokaisella varmenteella on myös vastakappale, **yksityinen avain**, joka varmenteen haltijan tulee säilyttää huolellisesti.
Varmennekortti (smart card with certificates)	Yksi tapa yksityisen avaimen huolelliseen säilyttämiseen on sijoittaa se toimikortille. Toimikorttia, joka sisältää haltijansa yksityisen avaimen ja varmenteen, sanotaan **varmennekortiksi**. Kun kortin haltija haluaa kirjautua tietojärjestelmään, hän laittaa varmennekortin kortinlukijaan ja antaa PIN-koodin. Väestörekisterikeskuksen sähköinen henkilökortti (poliisi antaa kansalaiselle), organisaatiokortti (työnantaja esim. yliopisto antaa työntekijälleen) ja mobiilivarmenteen sisältämä SIM-liittymäkortti (teleoperaattori antaa asiakkaalleen) ovat esimerkkejä varmennekorteista.

Varmentaja (certificate authority)	**Varmentaja** on organisaatio, joka antaa varmenteen. Uutta varmennetta tehtäessä varmentajan tärkeä tehtävä on huolehtia, että varmennekortti toimitetaan varmenteen haltijalle luotettavasti. Tämä tapahtuu tyypillisesti kasvotusten **rekisteröintipisteessä**, joka voi sijaita esimerkiksi yliopiston tiloissa. Tällöin varmentaja sopii yliopiston kanssa siitä, että yliopisto (esimerkiksi henkilöstöhallinto tai tietohallinto) vastaa rekisteröintipisteen toiminnasta. Jos varmennekortti hukkuu, varmenne mitätöidään asettamalla se **sulkulistalle**. Suomessa toimivia varmentajia ovat mm. Väestörekisterikeskus (sähköisellä henkilökortilla olevat kansalaisvarmenteet, organisaatiokortilla olevat organisaatiovarmenteet) ja Sonera CA (puhelimen liittymäkortilla olevat mobiilivarmenteet). Ulkomailla toimii lukuisia varmentajia. Yliopisto, jolla on riittävät taloudelliset ja tekniset edellytykset, voi myös rakentaa oman varmentajan.
Laatuvarmenne (qualified certificate)	Oman varmentajan voi pystyttää kuka tahansa asian harrastaja, mutta autotallissa toimivan varmentajan varmenteiden laadusta ei ole takeita. Laki sähköisestä allekirjoituksesta määrittelee **laatuvarmenteen**, jonka luotettavuudelle asetetaan erityisen korkeat vaatimukset. Laatuvarmenteen sisältävällä varmennekortilla tehty digitaalinen allekirjoitus rinnastetaan aina käsin tehtyyn allekirjoitukseen.
Väestörekisterikeskus	Väestörekisterikeskus on ainoa **laatuvarmentaja** Suomessa. Väestörekisterikeskus antaa laatuvarmenteita • sähköiselle henkilökortille (kansalaisvarmenteet) • matkapuhelimen liittymäkortille (kansalaisvarmenteet) • organisaatiokortille (organisaatiovarmenteet)
VRK:n organisaatio-varmenne	Väestörekisterikeskuksen **organisaatiovarmenne** on varmenne, jonka organisaatio hankkii ja kustantaa henkilölle (tyypillisesti: työnantaja hankkii työntekijälleen). Organisaatio järjestää myös rekisteröintipisteen, jossa organisaatiovarmenteen sisältämä **organisaatiokortti** annetaan oikealle henkilölle. Väestörekisterikeskus myöntää organisaatiovarmenteita ja -kortteja muun muassa virkamiehille valtion virastoissa, jolloin usein puhutaan **virkavarmenteista ja varmennekorteista**. Organisaatiovarmenteita voidaan myöntää myös yksityisten yritysten tai vaikkapa säätiömuotoisten yliopistojen henkilöille. Teknisesti ainoa ero näiden välillä on, että virkavarmenteessa varmenteenhaltijan organisaation kohdalla lukee viraston nimi, ei yrityksen nimeä.
Mobiilivarmenne	Luottokortin kokoisen toimikortin sijaan varmenne voidaan sijoittaa myös matkapuhelimen liittymäkortille, jolloin puhutaan **mobiilivarmenteesta**. Etuna mobiilivarmenteella on, että se ei tarvitse erityistä kortinlukijaa työaseman yhteyteen, vaan kirjautumishetkellä loppukäyttäjä antaa PIN-koodin matkapuhelimeensa, ja tunnistautuminen tapahtuu tekstiviestiliikenteenä matkapuhelinoperaattorin avulla. Väestörekisterikeskuksen organisaatiovarmenteista ei tällä hetkellä ole saatavilla mobiiliversiota.

12 Liite B: Esimerkki organisaatiovarmenteesta

```
$ openssl x509 -in matti_vanhanen.cer -inform der -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2000135416 (0x7737a4f8)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FI, ST=Finland, O=Vaestorekisterikeskus CA,
OU=Organisaatiovarmenteet, CN=VRK CA for Qualified Certificates
        Validity
            Not Before: Jul 26 05:35:52 2006 GMT
            Not After : Jul 20 21:59:59 2011 GMT
        Subject: C=FI, O=Valtioneuvoston kanslia/serialNumber=99736932C, GN=Matti,
SN=Vanhanen, CN=Vanhanen Matti 99736932C
                                    (1)
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:aa:ed:f8:8e:7e:94:84:26:51:1e:b8:f9:c9:21:
                    4e:af:7f:ee:b4:53:c4:74:96:cb:5d:a2:4c:49:69:
                    75:07:7e:76:06:28:eb:9e:53:db:c4:a6:bc:66:c0:
                    f5:5b:bc:d4:20:03:89:af:48:b1:78:29:aa:bf:52:
                    42:f4:89:5e:63:24:07:6e:8c:0f:11:0d:51:1e:dd:
                    91:1d:7d:2b:c9:b2:c3:15:80:71:4c:d3:ef:13:50:
                    ab:4c:1a:c8:89:51:f2:fd:57:fd:19:33:19:f4:40:
                    d7:5c:de:88:02:90:48:15:32:22:7d:1b:a0:d8:08:
                    67:db:21:12:cd:ff:24:1f:43
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
            CA:FALSE
            X509v3 Certificate Policies:
            Policy: 1.2.246.517.1.10.3.1
```

User Notice:
Explicit Text: Tutustu varmennepolitiikkaan - se certifikat policy
http://www.fineid.fi/cps2
CPS: http://www.fineid.fi/cps2/

Authority Information Access:
CA Issuers - URI:http://proxy.fineid.fi/ca/vrkqc.crt

X509v3 Subject Alternative Name:
email:matti.vanhanen@vnk.fi, othername:<unsupported>
(2)
Netscape Cert Type:
SSL Client, S/MIME
X509v3 Key Usage: critical
Digital Signature, Key Encipherment, Data Encipherment
(3)
X509v3 Extended Key Usage:
TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
(4)
X509v3 Authority Key Identifier:
keyid:54:1A:02:37:8F:8E:63:DF:8F:F0:30:23:4A:A8:FC:67:57:F0:53:A8

X509v3 CRL Distribution Points:
URI:http://proxy.fineid.fi/crl/vrkqcc.crl

URI:ldap://ldap.fineid.fi:389/cn%3dVRK%20CA%20for%20Qualified%20Certificates,
ou%3dOrganisaatiovarmenteet,o%3dVaestorekisterikeskus%20CA,dmdName%3dFINEI
D,c%3dFI?certificateRevocationList??objectClass=cRLDistributionPoint

X509v3 Subject Key Identifier:
F4:3E:EB:97:8C:00:05:00:05:2E:DF:FD:24:27:7F:76:B4:4A:7C:36
Signature Algorithm: sha1WithRSAEncryption
4a:34:1e:1d:23:83:a2:e1:76:ef:27:fb:13:77:5c:ed:6f:e7:
d2:dd:f0:36:c3:81:27:d7:c2:29:13:77:c3:eb:b5:76:1c:60:
92:f6:cc:84:ff:ed:a2:56:d7:37:89:6e:82:0c:bf:fb:d2:34:
4e:e1:5b:cc:b7:67:89:38:85:d0:14:f7:73:ca:dd:04:1a:e0:
8f:0a:d6:dc:8a:6c:4b:a4:2f:2b:f2:e7:9f:f1:ba:fd:01:90:
4c:6c:c2:11:bc:49:93:53:ea:fa:bb:75:4b:23:98:ee:3d:51:
1c:06:f6:97:12:43:19:ac:74:53:66:62:3d:37:15:7d:92:d4:
d2:1b:67:3a:fe:56:9d:e2:7b:08:d4:12:3c:d7:a8:09:4c:ff:
ca:29:1c:ea:d3:3c:e7:46:e1:31:dc:1d:b7:20:f9:d5:ef:fe:
10:ca:30:aa:16:71:6b:fb:de:ac:a6:13:8c:34:e6:79:7d:21:
37:2e:d5:36:5f:f5:9c:b8:f2:7e:c6:0f:0c:4e:8d:2e:b9:88:
27:b0:67:d3:8f:9f:9a:e0:6b:f0:47:6a:16:48:a3:6d:05:fe:
89:35:a8:77:5b:21:d8:52:cf:8c:09:93:8e:86:92:fb:3c:1b:
13:1a:56:80:c3:cb:b8:c4:aa:b0:0b:d3:e9:1e:6e:bf:e0:f6:
3f:d1:d6:7f

Varmenteen tietosisällöstä

(1) Tämän varmenteen haltija on Matti Vanhanen -niminen henkilö Valtioneuvoston kansliasta. Varmenteen tietosisällössä ei ole tehtävänimikettä, joten emme voi pelkästään varmenteen perusteella olla varmoja, kuuluuko se pääministeri Vanhaselle vai hänen mahdolliselle täyskaimalleen Valtioneuvoston kansliassa. Valtioneuvoston kanslian muista Matti Vanhasista varmenteen haltija yksilöidään sähköpostiosoitteen lisäksi sarjanumeron (99736932C) avulla, jolla kuitenkaan ei ole merkitystä ulkopuolisille.

(2) Myös sähköpostiosoite on yksilöivä tieto. Sähköpostiosoite talletetaan varmenteen Subject Alternative Name (SAN) –kenttään itse asiassa kahteen kertaan: ”email” sisältää turvapostissa käytetyn sähköpostiosoitteen, ja UPN (User Principal Name), jota OpenSSL-työkalu ei esimerkissä osannut tulkita (”<unsupported”>), on Windows-laajennus ja sisältää käyttäjän käyttäjätunnuksen Windows-toimialueessa. Väestörekisterikeskus on luvannut päivittää tietojärjestelmänsä niin, että nämä kaksi osoitetta eivät ole jatkossa automaattisesti samat.

(3, 4) Jokaiseen varmennekorttiin liittyy kaksi henkilövarmennetta; tunnistamis- ja salausvarmenne sekä allekirjoitusvarmenne. Varmenteen käyttötarkoituksista näemme, että tämä varmenne on tunnistamis- ja salausvarmenne, jonka avulla Vanhaselle voi lähettää salattua sähköpostia. Jos tämä olisi Vanhasen allekirjoitusvarmenne, olisi avaimen käyttötarkoituksena kiistämättömyys (non-repudiation).

Lisäksi Windows SmartCardLogin -käyttötarkoitus kertoo, että varmenne kelpaa Windows-toimialuekirjautumiseen.

13 Lähteet ja tausta-aineisto

Henkilön sähköinen tunnistaminen yliopistoissa ja ammattikorkeakouluissa - HSTYA-projektin muistio korkeakoulujen ylimmälle johdolle ja opetusministeriön virkamiehille. 2002.

Henkilötietolaki 1999/523.

Kaila, Urpo. Costs and benefits of strong authentication methods at NREN constituents. TERENA Networking Conference. http://tnc2008.terena.org/schedule/presentations/show.php?pres_id=61 . 2008.

Laki sähköisistä allekirjoituksista. 14/2003.

Laki viranomaisten toiminnan julkisuudesta 1999/621.

Opetusministeriön hallinnonalan tietohallintostrategia 2006–2015. Opetusministeriön julkaisuja 2006:52

Projektisuunnitelma. Varmennekortin ja varmenteiden käyttöönotto ja ylläpito yliopistoissa. Projektisuunnitelma. .28.9.2007

Sähköisen viestinnän tietosuojalaki (516/2004).

Tunnistuspalveluiden kehittäminen ja käyttö julkisessa hallinnossa..Valtiontalouden tarkastusvirasto:161/2008. 2008.

Tunnistaminen julkishallinnon verkkopalveluissa. VAHTI 12/06. Valtionhallinnon tietoturvallisuuden johtoryhmä. Valtiovarainministeriö.2006.

Yliopistojen Sec-ryhmän työvaliokunnan esitys opetusministeriölle. OpIT-info 4 / 26.4.2007: Varmennekorttien yhtenäisen käyttöönoton edistäminen Suomen yliopistoissa. 30.5.2007.

Valtionhallinnon salauskäytäntöjen tietoturvaohje. VAHTI 3/2008. Valtionhallinnon tietoturvallisuuden johtoryhmä. Valtiovarainministeriö. 2008.

Opetusministeriö

Undervisningsministeriet

Ministry of Education

Ministère de l'Education